2004-03

Information operations (IO) organizational design and procedures

Caldwell, Russell J.

Monterey, California. Naval Postgraduate School

NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

INFORMATION OPERATIONS (IO) ORGANIZATIONAL DESIGN AND PROCEDURES

by

Russell J. Caldwell

March 2004

Thesis Advisor:	Raymond Buettner
Second Reader:	Thomas Moore

Approved for public release: distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2004	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Information Operations (IO) organizational design and procedures.		5. FUNDING NUMBERS	
6. AUTHOR(S) Russell Caldwell			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		12b. DISTRIBUTION CODE	

13. ABSTRACT (maximum 200 words)

Multi National Force (MNF) operations recognize the existence of shared national interests in a specific geographic region. Furthermore, MNF operations seek to standardize some basic concepts and processes that will promote habits of cooperation, increased dialogue, and provide for baseline Coalition/Combined Task Force (CCTF) operational concepts. This thesis and its' recommendation for a Standard Operating Procedure (SOP) are aimed at improving interoperability and CCTF operational readiness. The SOP will focus on the spectrum of Information Operations (IO) with regards to Military Operations Other Than War (MOOTW) and Small Scale Contingencies (SSC) during MNF operations. First, existing doctrine and cases will be analyzed to develop a foundation for this study. This thesis will seek to identify the existing IO procedures to be utilized during MNF operations. Next, exercise observations and lessons learned reviews serve as the basis for IO SOP Annex development to support the MNF SOP.

14. SUBJECT TERMS: Multi National Force Information Operations, Military Operations Other Than War, Multi National Planning and Augmentation Team, Information Operations			15. NUMBER OF PAGES 179
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release: distribution is unlimited

INFORMATION OPERATIONS (IO) ORGANIZATIONAL DESIGN AND PROCEDURES

Russell J. Caldwell
Lieutenant, United States Navy
B.A., University of Kansas, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2004

Author:
Russell J. Caldwell

Approved by:
Raymond Buettner
Thesis Advisor

COL Thomas Moore, USA, PHD
Second Reader

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Multi National Force (MNF) operations recognize the existence of shared national interests in a specific geographic region. Furthermore, MNF operations seek to standardize some basic concepts and processes that will promote habits of cooperation, increased dialogue, and provide for baseline Coalition/Combined Task Force (CCTF) operational concepts. This thesis and its' recommendation for a Standard Operating Procedure (SOP) are aimed at improving interoperability and CCTF operational readiness. The SOP will focus on the spectrum of Information Operations (IO) with regards to Military Operations Other Than War (MOOTW) and Small Scale Contingencies (SSC) during MNF operations.

First, existing doctrine and cases will be analyzed to develop a foundation for this study. This thesis will seek to identify the existing IO procedures to be utilized during MNF operations. Next, exercise observations and lessons learned reviews serve as the basis for IO SOP Annex development to support the MNF SOP.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to extend my sincere thanks to Professor Ray Buettner, USN (Retired) and Col. Thomas Moore, PHD, USA for their guidance and encouragement as I worked toward accomplishing the monumental task of researching, editing, and completing this thesis. It was a privilege and an honor to work with them on this project.

I would also like to thank my parents, Jack and Diane, for the love, support, and encouragement they have given me throughout my educational pursuits. Above all, I want to thank my good friend, Elena, for standing by me as I embarked upon the journey of completing my Master of Science degree. Without your love and support, none of this would have ever been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. AREA OF RESEARCH

The U.S. Pacific Command (PACOM) continues to refine its Standardized Operating Procedures (SOP) to support Information Operations (IO) in a Multi National Force (MNF) structure. MNF operations recognize the existence of shared national interests in the region and seek to standardize some basic concepts and processes that will promote habits of cooperation, increase dialogue, and provide for baseline Coalition/Combined Task Force (CCTF) operational concepts.

This thesis is aimed at improving CCTF IO interoperability and operational readiness within the spectrum of Military Operations Other Than War (MOOTW) and Small Scale Contingencies (SCC). A complete and usable IO Annex for and MNF SOP does not exist and this research will produce a draft IO Annex that can be incorporated into future MNF operations to improve CCTF IO operations.

B. RESEARCH QUESTIONS

Given the complex operating environment of Mutli-National Operations, what are the appropriate standardized procedures for conducting MNF IO? What are the required contents of the IO Annex that will be required to enable successful IO MNF operations during MOOTW/SCC?

C. DISCUSSION

Information Operations, regardless of the operational context, seek to influence the decision making cycle of an individual, a group, or a nation. From full-scale conflicts to humanitarian efforts, U.S. military planners and operators have become aware that IO must be integrated and executed during the entire spectrum of conflict. During

military operations, IO must become an integral part of any operation. IO are essential to achieving full spectrum dominance. Since potential multinational partners will have varying levels of technology, a tailored approach to interoperability that accommodates a wide range or needs and capabilities is necessary.[1] Thus, when a cadre of military planners comes together to plan and execute IO operations during MNF operations, there is a need for standardized IO procedures to be cultural, psychological, economic, technological, informational, and political factors as well as transnational dangers that impact multinational operations.[2]

In order for IO to be effective during MOOTW/SCC operations a common foundation of understanding of IO must be provided. First of all, "Information warfare is about operations that target or exploit information resources".[3] For Pacific Command Multinational Planning and Augmentation Team (MPAT) and associated actors, the expanse of the information warfare battle space is critical. The battle space extends beyond the information realm; it also deals with the physical and information infrastructure, as well as the perceptual realm. The interactions of the three realms dealing with information content and process form the basic functional model of warfare.[4] The physical realms are the physical items that may be attack as a means to influence information. The information infrastructure realm deals with the information content or process that may be attacked electronically to directly influence the

[1] CJCS, JV 2020, 2000, pp. 23.

[2] CJCS, JP 3-16, 2000, pp. I-2.

[3] Denning, 1999, pp. 21.

[4] Waltz, 1998, pp. 27.

information process or content without physical impact on the target. The perceptual realms are attacks that may be directly targeted on the human mind through electronic, printed, or oral transmission paths.[5] Each realm associates a target with a means and a method of delivery to the target. From this model we can deduce that the source of transmission (the attacker), the transmission medium (the effects), and the receiver (the target) are the basic building blocks of the operational model of information operations and the foundation for effective IO.[6]

D. SCOPE OF THESIS

We will first discuss current U.S. IO policies, their limitations and benefits with regards to MNF operations. Next, the thesis will seek to identify the correct MNF IO procedures by reviewing existing doctrine, lessons learned, and case studies to develop the foundation for the MNF IO SOP Annex. Finally, we will offer a new MNF IO SOP Annex.

E. ROADMAP OF THESIS: A CHAPTER OUTLINE

Chapter I provides an introduction to the unique aspects of conducting Multi National Information Operations and the need for a usable IO SOP Annex to augment current U.S. IO policies and procedures.

Chapter II introduces the reader to U.S. IO policies, the competing policies, current interpretations, limitations, and causes of friction within the DoD with regards to Information Operations. This chapter will serve as the basis for introducing new IO procedures that will serve MNF operations in the future.

---

[5] Waltz, 1998, pp. 27.

[6] Waltz, 1998, pp. 149.

Chapter III provides the basic roadmap for the creation of the MNF IO SOP. Furthermore, it provides in-depth review of the limitations when conducting such operations, the key concepts required for understanding, the definitions, and elements of IO.

Chapter IV discusses the 1991 genocide in Rwanda from an information perspective and relates the shortcomings of current U.S. Joint IO procedures for the MNF environment in order to focus the reader on the need for correct IO procedures. Chapter V examines the interaction of the case study on Rwanda and how the IO Annex would be useful in future similar situations where mutli-national forces and IGO, NGO, and United Nations may be involved.

Chapter VI introduces the key concepts of the IO Annex in terms of Multi National Operations. The supporting IO reviews in Chapter II, the key ideas in Chapter III, and the case reviews will serve to support and structure the proposed IO Annex.

Chapter VII summarizes the study, the limitations of the thesis, and proposed follow-on research. Appendices include the IO Annex followed by a simple form to create IO offensive and defensive tasks. The final set of annexes will offer a series of questions to help planners and operators execute successful IO operations.

F. BENEFITS OF STUDY

The benefit of this study will help to identify, structure, and implement a viable Information Operations Cell Annex to support the SOP. IO is a constant evolving field of study. A solid baseline Annex will providing the basic framework and understanding of the unique challenges associated with operating in a MNF environment. MNF

planners will be able to continue the evolution of MNF IO Annex presented in this study. It will give operators and planners the ability to quickly and effectively review and implement IO during Crisis Action Planning (CAP) or deliberate planning to support MOOTW/SCC. Second, the study will identify the problems, drawbacks, and conflicts that may arise when cadres of military planners from various nations rapidly augment a MNF headquarters to support IO during MOOTW and SSC. If these factors are isolated prior to operations, they may be avoided during MNF planning phases.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CURRENT IO POLICIES

> *Take your spears, clubs, guns, swords, stones, everything. Sharpen them, hack them, those enemies, those cockroaches. Hunt out the Tutsi. Who will fill up the empty graves? There is no way the rebels should find alive any of the people they claim as their own…*
>
> -Radio Television Libre des Milles Colines[7]

A. INTRODUCTION

Information warfare, (i.e., Information Operations) as a separate technique of waging war, does not exist.[8] Even in the U.S. military there is some disagreement and confusion regarding the scope of I.O. For instance, the U.S. Air Force maintains that Information Operations are a subset of information warfare, and deals exclusively with the use of military information functions. Information operations do not include actions to deny, corrupt, or destroy the enemy's information or efforts to protect ourselves against those actions.[9] On the other hand, the CJCS maintains that IO does deny, corrupt, or destroy enemy information.[10] Though definitional differences are apparent in the literature, for this work IO definitions will focus on the need to influence a leader, group, or information structure while protecting one’s own decision making processes. However, for the MPAT organization working through PACOM, a new definition for the SOP was created to standardize operations. Thus, the need to introduce and summarize the

---

[7] Adams, 1998, pp. 272. *Note: Adopted from Free Radio-Television of the Thousand Hills or Radio Hate of the Hutu tribe that killed thousands of Tutsi people in 1994.*

[8] Libicki, 1996, pp. x.

[9] DOAF, 1995, pp. 3.

[10] CJCS, JP 3-13, 1998, pp. viii.

current MPAT definition and how it was created is key to understanding the implication of the IO Annex.

B. JOINT U.S. IO POLICY REVIEW

The current and most widely accepted IO definition is, "IO involve actions taken to affect adversary information and information systems while defending one's own information and information systems. IO applies across all phases of an operation, throughout the range of military operations, and at every level of war".[11] All phases of an IO operation apply to peace through war and eventually restoration procedures.

Originally the MPAT definition was adopted directly from the current U.S. definition. Almost immediately, MPAT members found that the definition was too broad in scope because it failed to define what constitutes an information system. MPAT planners required a more precise definition in order to have the ability for planners from multiple countries find a common understanding of the scope of IO. For example, the goal of MPAT is, "to enhance regional cooperation and multinational force readiness for crisis response".[12] This statement indicates the MPAT will be called in after the earthquake, or after hostilities have begun, or during the need for large scale humanitarian operations are required. Thus the spectrum of operations regarding the current U.S. definition comes into question. If the SOP is to be used by numerous countries that have limited interaction and experience with IO operation, the ability for MPAT planners to quickly and efficiently reference the IO Annex is crucial when limited by time,

[11] CJCS, JP 3-13, 1998, pp. vii.

[12] MPAT SOP, 2002, pp. IV.

space, and force during operations. Thus the definition of IO requires small but important changes.

C. MPAT IO DEFINITION

The current MPAT IO definition created via the inputs of senior officers from nations with Asian Pacific interests is, “Information Operations (IO) are actions taken to effect information, information systems, and influence decision making processes of political, military, and social entities while protecting one’s own. IO spans the entire spectrum from peace, to crisis, to conflict, to restoration”.[13] MPAT participants created the definition to increase the understanding of the factors and the entities involved with IO. They felt the need to draw out the key phrase of “decision making processes of political, military, and social entities” because this would focus the IO cell on the process of information within the decision making cycle.

The Joint US definition was changed based on two problems encountered during MPAT conferences. First, the current Joint US definition assumes the planners understand that information systems target information or information systems in order to affect the information-based process weather human or automated, including the decision makers of the opposing force.[14] However, relying on interactions with senior officers of MPAT nations it became apparent that their interpretation of the US policy on IO created the feeling that IO only focuses on the technological aspects of military information operations. In order for MPAT planners to execute IO, the need to draw out the idea

[13] MPAT SOP, 2002, pp. V.

[14] CJCS, JP 3-13, 1998, pp. 30.

that IO can influence, destroy, degrade, or mislead the leadership and not only the technology associated with the opposition was crucial for the creation of the IO SOP.

Second, the term “adversary” was removed from the MPAT definition because MPAT planners felt that it implied that IO would always target the enemy or the aggressor during operations. For instance, US Joint publications state that although strategic offensive IO targeting may involve direct, indirect, and supporting attacks, most strategic targeting will involve direct attacks on the information and information systems within the elements of national power that will cause an adversary or potential adversary to make decisions favorable to US interests.[15] The goal of MPAT is not to be involved in major conflicts where there is a clear separation of “good guys and bad guys” and major military operations are ongoing or unavoidable. Their focus is MOOTW.

The MPAT organization understands and assumes that IO may be used against the entire population during MOOTW/SCC operations. For example, during such operations a “host nation” is designated. The host nation is a nation in which CCTF forces are present because of government invitation or international agreement to conduct CCTF operations or stage CCTF forces to provide support to another country.[16] The MPAT organization understands and assumes that IO may be used against the entire population of the host nation during MOOTW/SCC operations. This implies that IO might possibly be used against their own population and the feeling of the term “adversary” may have unforeseen and

[15] CJCS, 1998, JP 3-13, pp. II-14.

[16] MPAT SOP, 2002, pp. B3 A-1.

negative implications against the entity they wish to influence. Furthermore, the need for the definition to take on a less aggressive tone was required. The MPAT definition attempts to imply a more peaceful type of influence operation to meet mission objectives with-in the cultural and legal limitations of the operation.

For the creation of the definition and eventually the IO Annex, a basic IO model was used. Waltz describes IO as, “Information Operations that are performed in the context of a strategy that has a desired objective (or end state) that may be achieved by influencing a target (the object of influence)”.[17] His model of IO focuses on three levels. The first level of the model is the perceptual or psychological level and is aimed at management of the perception of a target audience. The second layer is the information infrastructure layer that accepts, processes, manages, and stores the information. The final layer is the physical system level, which includes the computers, physical networks, telecommunications and supporting structure components that implement the information system. All three of the layers can be attacked or defended with one or more elements of information operations. Table 1 summarizes Waltz’s characteristics of the Operational Model of Information Operations and serves as the backbone for the creation of the IO Annex.

[17] Waltz, 1998, pp. 148.

Model Layer	Characteristics and Components	Attacker's Operations	Defender's Operations	Desired Effects
Perceptual	**Knowledge and understanding in human space:** • **Perception** • **Beliefs** • **Reasoning**	**PSYOPS** **Diplomacy** **Civil and public affairs**	**Psychological security** **Objective aids**	**Cognitive-influence decisions and behavior**
Infrastructure	**Information maintained in cyberspace:** • **Data structures** • **Processes** • **Protocols** • **Data content**	**Network attack, support measures** **Electrical power attack**	**INFOSEC information security**	**Functional-influence the effectiveness and performance of information functions supporting perception, controlling physical processes**
Physical	**Data managed in physical space:** • **Computers** • **Storage** • **Networks** • **Electrical power**	**Physical electronic attack** **Intrusion** **Theft** **Wiretapping** **Destruction**	**OPSEC physical security**	**Technical – affect the technical performance and capacity of physical systems**

Table 1. CHARACTERISTICS OF THE OPERATIONAL MODEL OF INFORMATION OPERATIONS[18]

[18] Waltz, 1998, pp. 150.

D. KEY CONCEPTS

IO spans the entire spectrum of military operations from peace to restoration. However, for the creation of the IO SOP, the MPAT organization focused on MOOTW/SCC operations. The limited scope in the nature of operations is due to MPAT Operational Start Points. The Operational Start Points outlined in the SOP are the foundation for a MNF per forming rapid activation of CCTF HQs to provide effective mission accomplishment. Thus, nations can use the SOP in a variety of ways: (1) This SOP can act as an additional reference to existing national SOPs; (2) It can be integrated into existing SOPs; or, (3) This SOP can be used as the national CCTF SOP. This SOP is not intended to be a directive; rather, it acts as a guide upon which to base dialogue and planning. It is not designed to support a Major Regional Conflict.[19]

The MNF focus is to promote stability and peace and/or support non-military options during MOOTW/SCC. However, this is not to imply that the CCTF does not maintain the right to self-defense or may not have to resort to military action, peacekeeping, peace enforcement, or even to fight and win in a small-scale conflict. Also, the possibility does exist that the MPAT may be drawn into a full-scale regional conflict or war. IO planners must be ready for this possibility. The IO Annex is based on those principles of MOOTW/SCC operations found in Figure 1.

[19] MPAT SOP, 2002, pp B-1.

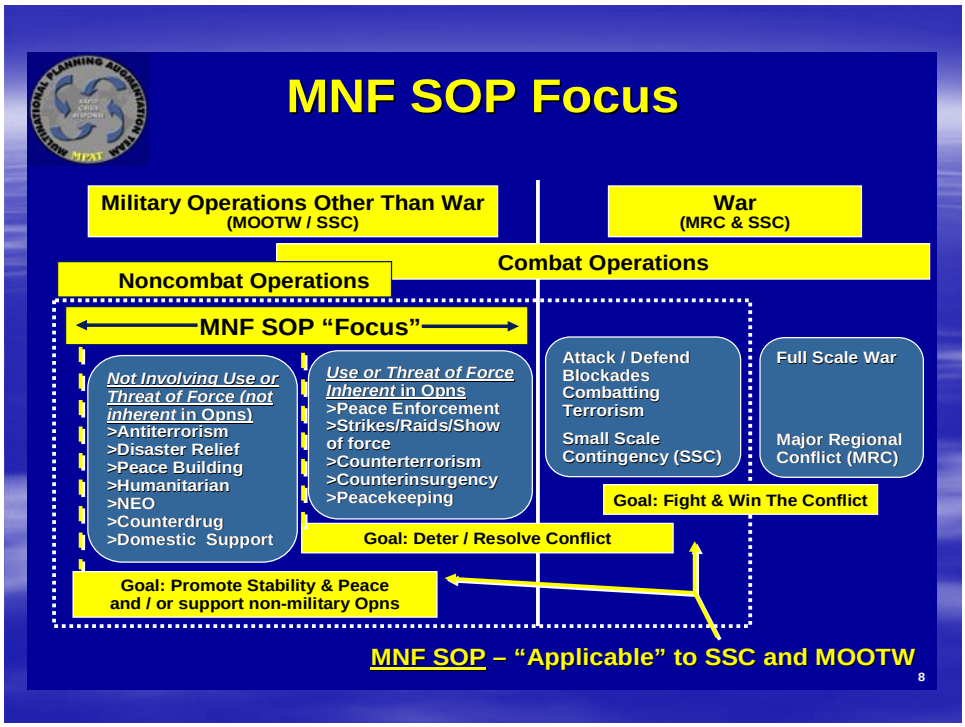

Figure 1. MNF SOP FOCUS[20]

Figure 1 suggests clear distinctions between War and MOOTW, and further divides MOOTW operations by the terms "Not involving use or threat of force" versus "Use or threat of force". In reality, such distinctions may be unclear and can shift rapidly. In the end, a military's basic function is to have the ability to use force to impose its will on an adversary. As such, MNF forces working within the ranges of MOOTW must be able to rapidly shift to the use of force or threat of force to ensure mission accomplishment. For example, Peace Keeping Operations (PKO) can transit quickly to Peace Enforcement Operations (PEO) because threat forces escalate their level of operations against the coalition. The MNF must be ready

[20] MPAT SOP, 2002.

to fight (or transition to combat) at all times. All MNF planning and execution actions must assure this.[21]

1. Elements of Military Operations Other Than War (MOOTW) related to MPAT Operations

Military Operations Other Than War (MOOTW) are operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power and can occur before, during, and after war. MOOTW supports the deterrence of war, resolution of conflict, promotion of peace, and civil authorities in response to domestic crises, to include relief of human suffering and recovery from national disasters. MOOTW falls into three environments; permissive, hostile, and uncertain.[22] IO planners must have a basic understanding of the three MPAT environments of MOOTW and understand how to tailor IO using the SOP in order to conduct effective IO.

The permissive environment includes those in which the host country military and law enforcement agencies have control and the intent and capability to assist the CCTF operations and maintain civil order. This environment will include IO actions against or in support of:

(1) Peacekeeping Operations
(2) Antiterrorism (part of Combating Terrorism)
(3) Freedom of Navigation (air and maritime)
(4) Counter drug Support
(5) Humanitarian Assistance (HA)
(6) Disaster Relief (DR)
(7) Protection of Shipping
(8) Nation Assistance Programs
(9) Noncombatant Evacuation Operations (NEO)
(10) Arms Control

[21] MPAT SOP, 2002, pp. A1-B1.

[22] MPAT SOP, 2002, pp. B7-1.

(11) Recovery Operations

For instance, in 2001 massive earthquakes and aftershocks rumbled through western India that killed thousands of people and flattened towns and villages throughout Gujarat state. Immediately the United Nations, U.S. Pacific Command, American Red Cross, and numerous private organizations sent personnel and disaster relief items to help India deal with massive destruction and immediate relief. For example, the USS Cowpens (CG 63) delivered more than $50,000 of earthquake relief supplies to India. These efforts are part of the U.S. Pacific Command's mission of promoting peaceful development in the Asia-Pacific region through humanitarian assistance and disaster relief.[23] The IO operation was simply to state the good intentions of the agencies involved and indicate to local citizens that the international community was there to help. These types of actions clearly fall into the permissive environment, the host nation requested and received immediate help, and the Indian government was in control of the situation and was able to support international humanitarian relief operations.

MOOTW operations in a hostile environment are those in which hostile forces have control and the intent and capability to effectively oppose or react to CCTF operations. The CCTF operational goal is to deter war and resolve the conflict. Examples of such operations are:

(1) Peace Enforcement (PEO) (part of Peace Operations)
(2) Counterterrorism (part of Combating Terrorism)
(3) Noncombatant Evacuation Operations (NEO) (hostile)
(4) Enforcement of Sanctions / Maritime Intercept Operations

[23] PACOM, 2001.

(5) Enforcing Exclusion Zones
(6) Ensuring Freedom of Navigation and Over flight
(7) Show of Force Operations
(8) Raids and Strikes
(9) Recovery Operations (hostile)

The third environment is the uncertain environment. MOOTW in the uncertain environment is one in which the control, intent, and capability of host nation and hostile forces are unknown or uncertain. The type of IO required may also be uncertain. The CCTF must be prepared to operate in either a permissive, hostile, or uncertain environment.[24] The distinction between the hostile or uncertain environment may not clear. For instance, Multinational humanitarian and military efforts such as those seen in Somalia, Kosovo and Afghanistan are known as Complex Humanitarian Emergencies. These types of emergencies are complex and difficult to operate in because they contain political, military and humanitarian considerations.[25] Furthermore, it is not always clear how the host nations, factions, or the entities that control a given state or situation may react to multinational forces present in the AOR.

In Somalia, for example, four distinct elements led to the conflict between UN/US forces and the Somalis in an uncertain environment. These key elements were (1) the Somali culture and character, (2) the impact of the legacy left by the dictator Siad Barre on the psyche and ambitions of the Somali clans, (3) the tainted relationship between the UN leadership and the Somali people, and (4) the

[24] MPAT SOP, 2002, pp. B7-4.

[25] Barge, Davis, Schwent, 2003, pp. v.

failure of the US and UN leaders to effectively deal with the most powerful and influential Somali warlord, General Mahammad Farah Aideed.[26] Prior to and during operations, the inability of coalition forces to differentiate between who controls what, when, and where led international forces to assure a hostile environment upon arrival. The hostile environment developed into an uncertain environment. The uncertain environment proved to be extremely dangerous for all sides and led to UN/US mission failure as coalition forces became embroiled in factional disputes.

During MOOTW in any pre-defined environment will focus on the issue of CCTF legitimacy. Legitimacy is a perception by a specific audience of the legality, morality, and/or rightness of a set of actions. Operations may be strictly legal but may not be accepted as legitimate. The audience can be the participating nations' people, host nation personnel, affected nation personnel, coalition forces, National Government Organizations International Organizations, or other factions involved in the crisis. If operations are perceived as legitimate, then CCTF IO is likely to have strong support. If not perceived as legitimate, actions may not be supported are more likely to be actively resisted by friendly and enemy elements and factions.[27]

2. Elements Of Information Environment/Management Related To MPAT Operations

The Information Environment (IE) is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. Information Management (IM) is all

[26] Norquist, 2002.

[27] MPAT SOP, 2002, pp. B7-5.

activities involved in the collection, filtering, fusing, processing, dissemination and use of information for CCTF operations. Information that promotes understanding of the battle space enables commanders to better formulate and analyze courses of action, make decisions, execute those decisions with adjustments to the plan as necessary, and accurately assess the operation.[28]

A disciplined, streamlined Information Management (IM) system allows decisions to be executed (and feedback to flow) more efficiently and effectively. The focus of the IO staff must be on what the CCTF needs, when they need it, and presenting it in a usable format to support their planning, decision, execution, and assessment cycle. Integration of MNF participating nations within mature CCTF IM systems can present many challenges. Integration may be easy for some multinational participants and it may be a challenge for others. Unity of effort, clear and concise communications and information exchange must be the operative principles for multinational operations. The five crucial dimensions for measuring the quality of information available within the CCTF are:

(1) Completeness: Are all the relevant items available, including entities, their attributes, and relationships between them.

(2) Correctness: Are all the items in the system faithful representations of the realities they describe.

(3) Currency: Age of the items of information, often termed their latency.

(4) Accuracy or Level of Precision: Which is conditional on the purpose the user has in mind.

[28] MPAT SOP, 2002, pp. C8-2.

(5) Consistency: Across different command centers, functionally specialized areas, and applications.[29]

To enhance the IM system and the military utility of the information, the CCTF must acquire the right data, optimize the extraction of knowledge, distribute and apply the knowledge, and ensure the protection of the information. The objective of each of these actions is to refine the information processes to optimize the exploitation of available data and distribution of knowledge to appropriate users.[30] The degree of IM system maturity within the CCTF will be dependent upon the national capabilities and training levels of the participating nations' forces. Some nations' forces will be fully capable and trained in modern day information technologies, while other nations' may be less capable and not trained. Regardless of any differences in capabilities, an IM system must be developed that supports the CCTF's needs and the needs of component commanders. The four categories of the IM for MPAT to support IO must include:

(1) Acquire the Right Data: The type, quality, accuracy, timeliness, and rate of data collected have a significant impact on knowledge delivered.

(2) Optimize the Extraction of Knowledge: The process of transforming data into knowledge may be enhanced or refined to improve efficiency, throughput, end-to-end speed, or knowledge yield.

(3) Distribute and Apply the Knowledge: The products of information process must be delivered to users on time, in understandable formats, and in sufficient quantity to provide useful comprehension to permit actions to be taken.

[29] Alberts, Garstka, Hayes, & Signori, 1995, pp.84.

[30] Waltz, 1998, pp. 73.

(4) Ensure the Protection of Information: In the competitive and conflict environments, information and the collection, processing, and distribution channels must be protected from all forms of attack to secure reliability for and availability to the user.[31]

CCTF IM will be focused on providing quality information to support CCTF decision-making. The goal of IM is to provide a timely flow of relevant quality information, enabling the CCTF and staff to anticipate and understand the consequences of changing conditions. IM directs the processes through which information is collected, processed, analyzed, and disseminated. Users establish the information requirements. IM is performed at all levels, regardless of the extent of automation. The principles of IM apply in every situation in which a decision is made.[32]

E. KEYS OF INFORMATION OPERATIONS RELATED TO MPAT OPERATIONS

Units or cells of information warriors will conduct the information operations that require coordination of technical disciplines to achieve operational objectives. These cells require the support of planning and control tools to integrate and synchronize both the defensive and offensive disciplines.[33] Each cell that is created when the rapid activation of a CCTF HQs is required, must understand the basic elements of IO in order to be successful. Furthermore, Commanders of the CCTF HQ also require a basic framework for managing and monitoring the IO practices of the CCTF IO Cell. The paragraphs that follow give an introductory view of the elements of IO and how each one

[31] Waltz, 1998, pp. 73.

[32] MPAT SOP, 2002, pp. C8-2.

[33] Waltz, 1998, pp. 229.

relates to the MPAT SOP to support successful completion of operations within the CCTF.

1. Offensive Information Operations

Offensive Information Operations are malevolent acts conducted to meet strategic, operational, or tactical objectives. The operations may be performed covertly, without notice to the target, or they may be intrusive, disruptive, and even destructive. The effects on information may bring physical results that are lethal to humans.[34] Offensive IO involves the integration and orchestration of varied capabilities and activities into a coherent, seamless plan to achieve specific objectives.[35]

To achieve effective offensive IO, a source of action must be assigned. For MPAT planners, supporting capabilities and activities that can be integrated to conduct offensive IO include the same capabilities and processes that traditionally support C2W, OPSEC, PSYOP, military deception, EW, and physical attack/destruction. Additionally, Computer Network Operations (CNO) may be considered for development and integration in offensive IO.[36]

Offensive information operations can be a single attack or a larger operation or campaign that involves multiple attacks.[37] It is useful to categorize and compare different types of operations. For the IO SOP, a summary of offensive IO in Table 2 is included to help MPAT planners

[34] Waltz, 1998, pp. 251.

[35] CJCS, JP 3-13, 1998, pp. II-1.

[36] CJCS, JP 3-13, 1998, pp. II-3.

[37] Denning, 1999, pp. 30.

understand exactly what are the tools and potential benefits or outcomes of offensive IO.

Outcome	Category/Operation	Note:
Increased Availability to Offensive Player	Collection of Secret Information	Espionage and Intelligence Operations, OSINT, HUMINT, SIGINT, IMINT, Competitive Intel, Economic Intel
	Information Piracy	Copyright or trademark violations
	Penetration into Physical Premises and CS	CNO, Spies
	Superimposition Fraud	Unauthorized access to an information resource
	Identity Theft	Fraudulent use
	Physical Theft	Such as printed documents
Decreased Availability to Defensive Player	Physical Theft	Such as printed document, disks
	Sabotage	Physical, electronic, and software attacks, jamming, physical destruction, DNS
	Censorship	Denies access to information sources
Decreased Integrity	Tampering	Alter the contents of Information resources
	Penetration	Cover intrusions into the information space
	Fabrication	Create false information

Table 2. OFFENSIVE INFORMATION WARFARE OPERATIONS[38]

[38] Denning, 2002, pp. 33. *Author's Note: Selection and employment of specific offensive capabilities against an adversary must be appropriate to the situation and consistent with CCTF objectives.*

The targets of offensive IO fall into three distinct categories: the global information infrastructure (GII), national information infrastructure (NII), and the defense information structure (DII). The GII includes the international complex of broadcast communications, telecommunications, and computers that provide global communications, commerce, media, navigation, and network services between the NIIs. The NII includes the subset of the GII within a nation, and the internal telecommunications, computers, intranets, and other information services not connected to the GII. The DII includes the infrastructure owned and maintained by military organizations for purpose of national security.[39] For additional clarification, the MPAT planners felt within the three categories additional information was required when deciding on targeting fo offensive IO:

(1) Leadership: including civilian, social, military, and cultural targets.

(2) Military Infrastructure: including communications, intelligence, logistics, operations, and weapons systems.

(3) Civil Infrastructure: including telecommunications, transportation, energy, economic, and manufacturing.[40]

Offensive IO gives the CCTF Commanders the ability to attack and influence the information environment during all phases of the operation. However, over a wide range of

[39] Waltz, 1998, pp. 173.

[40] *Author's Note: These actions must be permissible under the law of armed conflict, consistent with applicable domestic and international law, and in accordance with applicable rules of engagement.*

offensive IO capabilities, means of delivery, and targets available to CCTF IO Cells, they will encounter limitations. Limitations associated with time, space, force, risk, and legal implications all impact operations. These limitations will be discussed in detail in Chapter III.

Offensive IO can utilize physical destruction. Currently, in the U.S. military there is a turf war regarding the operations domain for the physical destruction of targets. Thus, current policies have taken the physical destruction domain of operations out of IO and returned responsibility to the traditional war fighter, not the information warrior. However, IO planners must understand that the physical destruction of a target can accomplish or hinder the IO plan on the strategic, operational, or tactical level. The IO Annex indicates that an IO Cell representative must be present at targeting boards that deal with physical destruction of a target to ensure IO targets are not compromised.

When dealing with offensive IO, the CCTF should focus on the precision engagement. Precision engagement is the ability of joint forces to locate, surveil, discern, track objectives or targets, select, organize, and use the correct systems. It focuses on the ability of the force to engage with decisive speed and overwhelming operational tempo as required, throughout the full range of military operations. The key to precision engagement is to link the sensors, delivery systems, and effects during joint force operations.[41] Offensive IO can be enhanced with precision engagement because IO has the capabilities to identify and

[41] CJCS, JV 2020, 2000, pp. 22.

locate critical nodes and targets for the CCTF. It has the ability to engage with electronic or psychological forces.

2. Defensive Information Operations

Defensive Information Operations are those actions that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.[42] Since it is a practical impossibility to defend every aspect of the infrastructure and every information process, defensive IO ensure the necessary protection and defense of information and information systems upon which joint forces depend to conduct operations and achieve objectives. [43]

For effective defensive IO, the six basic components and capabilities described by Waltz are critical to mission success. When the CCTF requires protection of their information systems and operations, they must focus on issues associated with availability, integrity, authentication, confidentiality, nonrepudiation, and restorations of each system. Availability provides assurance that information, services, and resources will be accessible and usable when needed by the user. Integrity assures that information and processes are secure from unauthorized tampering. Authentication assures that only authorized users have access to information and services on the basis of controls. Confidentiality protects the existence of a connection, traffic flow, and information

[42] Waltz, 1998, pp. 301.

[43] CJCS, JP 3-13, 2000, pp. III-1.

content from disclosure to unauthorized parties. Nonrepudiation assures that transactions are immune from false denial of sending or receiving information by providing reliable evidence that can be independently verified to establish proof of origin and delivery. Restoration assures information and systems can survive an attack and that availability can be resumed after the impact of the attack.[44]

For the CCTF to safeguard information and resources it may secure them behind a physical or digital lock.[45] The physical lock includes locks and keys. The CCTF must ensure that access and accountability for such systems is monitored and periodically reviewed. The use of cryptography within the CCTF can help ensure the security of electronic information. Other critical assets that should be available to the MPAT are digital ciphers, the generations and distribution of electronic keys, stenanography, anonymity, sanitations and the correct disposal of critical information.[46] These methods of protecting and destroying electronic and physical forms of information help limit the availability of information to opposing forces. Most nations practice some form of information gathering against adversaries and friends in the form of espionage and general information gathering from open or closed sources. To fail to protect information in any one form may not jeopardize operations, however the inability of the MPAT to protect a combination of information assets may cause mission failure.

---

[44] Waltz, 1998, pp. 302.

[45] Denning, 1999, pp. 285.

[46] Denning, 1999, pp. 287.

Four interrelated processes comprise defensive IO; information environment protection, attack detection, capability restoration, and attack response.[47] First, protection of the information environment is a combination of information systems and facilities. The protection of personnel and physical security will help ensure the information environment can operate effectively because this procedure contributes to information assurance. This protection also applies to any information medium or form, including hard copy, electronic, magnetic, video, imagery, voice, telegraph, computer, and human systems. Second, the ability for the CCTF IO Cell to detect attacks in a timely manner will initiate the ability to restore the system and possible counter attack if needed. Capability restoration relies on established procedures and mechanisms for prioritizing restoration of essential functions. The use of Computer Emergency Response Teams (CERT), technical restorations, automated intrusion detection; inventory of systems resources, and post-attack analysis will provide the CCTF effective defensive IO because these methods indicate potential shortcomings and gaps in information security and management. Finally attack response is validation that an attack is complete. This allows the CCTF to trigger an IO response. Elements of the IO response can include electronic attack, law enforcement, diplomatic actions, sanctions, and military force.[48]

Defensive IO must go beyond the technical protection of information and information systems. For the CCTF it must maintain the ability to protect members from the

[47] CJCS, JP 3-13, 1998, pp. III-1.

[48] CJCS, JP 3-13, 1998, pp. III-14.

information message and counter propaganda. For instance, in the summer of 1994 the world stood by and watched as the airwaves of Rwanda urged the mass killings of Tutsi people by a rival tribe the Hutu. Hutu extremists used simple mobile radios to urge their people to go on mass killing sprees.[49] Men, women, and children were raped, tortured, and killed. The world may never know the true extent of the killings. A simple application of electronic warfare and jamming airwaves could have prevented the slaughter.[50] It is imperative that defensive IO procedures in the CCTF address adversary counter propaganda and its sources be neutralized quickly.

For defensive CCTF IO the theory of "Full Dimensional Protection" should be adopted. Full dimensional protection is the ability of the joint force to protect its personnel and other assets required to decisively execute assigned tasks. Full dimensional protection is achieved through the tailored selection and application of multilayered active and passive measures, within the domains of air, land, sea, space, and information across the range of military operations with an acceptable level of risk.[51] To ensure successful defensive IO operations, the CCTF must ensure information superiority is obtained through full dimensional protection coupled with precision engagement within the AOR.

3. Psychological Operations (PSYOP)

Psychological operations are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective

[49] Adams, 1998, pp. 273.

[50] *Author Note: An in-depth Rwanda case study is included in Chapter 4.*

[51] CJCS, JV 2020, 2000, pp. 26.

reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.[52] PSYOP units should be integrated into all multinational operations. The multinational force commander must ensure that all PSYOP activities, regardless of national origin, are coordinated because the world's almost instantaneous access to news and information makes it nearly impossible to localize any information campaign. For instance, a psychological leaflet handed out in Bosnia is just as likely to be shown by a reporter on the nightly news in the United States or Europe as it is to be read in Sarajevo. This can lead to an uncoordinated effort in various regions around the world, where the government's information dissemination power is not used to its fullest advantage. In addition, contradictory information themes could be broadcast simultaneously through the various venues resulting in reduced effectiveness.[53]

PSYOP must begin early, preferably before deployment, to prepare a population for the arrival of multinational forces and develop communication channels that can be used from day one of an operation.

[52] CJCS, JP 1-02, 2003, pp.viii.

[53] DSB, 2000.

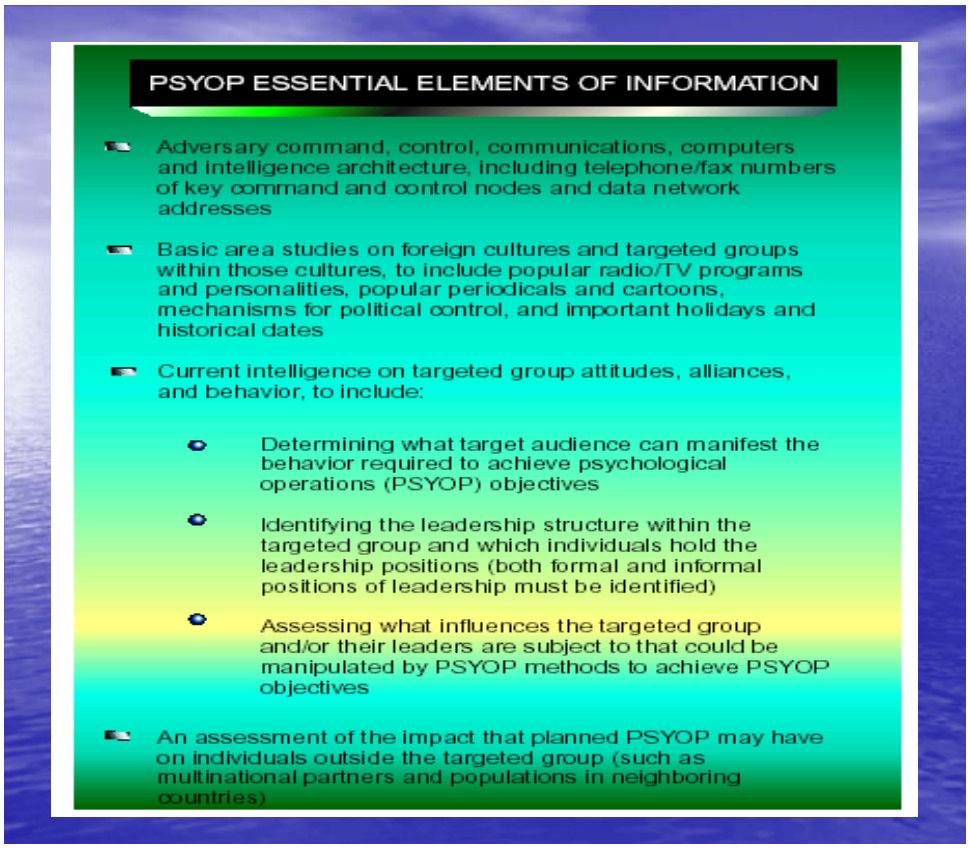

Figure 2. PSYOP ESSENTIAL ELEMENTS OF INFORMATION[54]

PSYOP provides the commander with controlled channels to communicate with all elements of a population: civilians, military, or belligerent factions. PSYOP communicate policy, provide information, and can persuade groups to cooperate with multinational forces. A detailed analysis of a country's culture, religion, political climate, and military organization can help the multinational force commander to effectively apply PSYOP to communicate policy, provide information, and persuade groups to cooperate with friendly forces.

When the Armed Forces of the United States are integrated into a multinational command structure, peacetime PSYOP policies and wartime conduct should be

[54] CJCS, JP 1-02, 2003.

coordinated and integrated to the maximum extent possible for the attainment of U.S. and multinational security objectives. However, U.S. PSYOP normally will be approved in U.S. channels regardless of the composition of the multinational force chain of command.[55] This contradiction between the integration and authorization of PSYOP themes may cause unforeseen problems. Attempts to minimize these contradictions must be addressed in the actual chain-of-command structure within the CCTF. For instance, each nation furnishing forces to the CCTF establishes a National Command Element (NCE) within the CCTF command. Normally this person is the senior officer in the CCTF for a given nation. This establishes the national command link back to respective nations' national authorities.[56]

The PSYOP model used to create the MNF IO SOP follows the U.S. Joint Publication on PSYOP. Each type of PSYOP is categorized into strategic, operational, or tactical level psychological operations. Strategic level PYSOP is conducting international information activities to influence foreign attitudes, perceptions, and behavior in favor of US goals and objectives. Next operational level PYSOP activities are designed to strengthen U.S. and multinational capabilities to conduct military operations in the operational area and accomplish particular missions across the range of military operations. Tactical level psychological operations outline how military force will be employed against opposing forces to attain tactical

[55] CJCS, JP 3-53. 2003 pp. VI-14.

[56] *Author's Note: Chapter III will present an in-depth review of the COC.*

objectives. Figure 3 summarizes military psychological operations.[57]

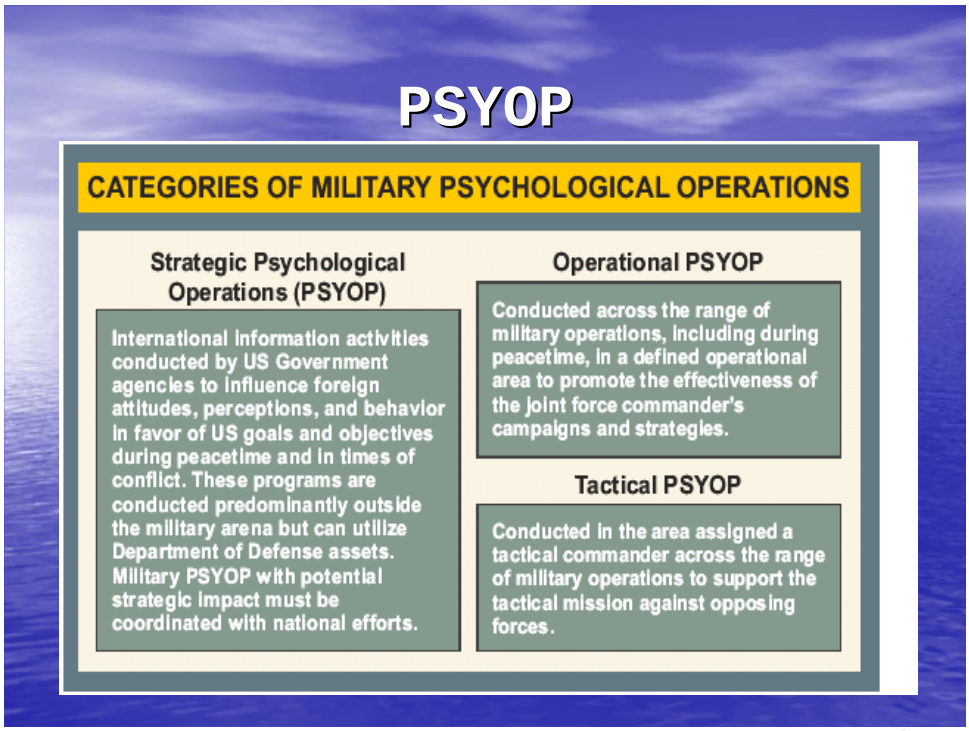

Figure 3. MILITARY PSYCHOLOGICAL OPERATIONS[58]

During operations, PSYOP are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The definition could also be labeled propaganda. Normally, propaganda is actions against the coalition and psychological operations are actions against the IO target. Regardless of how they are labeled, the effects and process are the same.

[57] CJCS, JP 3-53, 2003, pp. I-4.

[58] CJCS, JP 1-02, 2003.

4. Military Deception (MILDEC)

Military deception are actions executed to deliberately mislead military decision makers as to friendly military capabilities, intentions, and operations, thereby causing them to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are:

(1) Strategic Military Deception: Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations.

(2) Operational Military Deception: Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater to support campaigns and major operations.

(3) Tactical Military Deception: Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements.

(4) Service Military Deception: Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems.

(5) Military Deception in Support of OPSEC: Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract

> foreign intelligence away from, or provide cover for, military operations and activities.[59]

Military deception is extremely useful during all operations. For instance, on the eve of World War II, the Red Army at Khalkhin Gol, commanded by General Zhukov, developed an elaborate deception plan against the Japanese forces in a major Manchurian border battle in August 1939. After a significant border incursion and clash, Zhukov's deception measures "were aimed at creating the impression that we were making no preparations for an offensive operation." Consequently, troop concentrations and redeployments were done at night, radios and telephones were used to pass false information, and attack groups were moved to their jumping-off positions shortly before the attack. Deception efforts and diversionary attacks served to cloud the Japanese estimate of Soviet activities and keep the Japanese assessment off-balance. According to the Kwantung Army command, "We had no prior clue from intelligence at any level, from the front to army headquarters, to lead us to expect there would be an offensive on such a scale at this time."[60] The Soviets achieved operational surprise when Red Army forces swiftly surrounded the awed Japanese forces and completely destroyed their units.

Recognition of the vital role that deception of all kinds plays in military operations is clearly evident in the Joint Chiefs of Staff Memorandum of Policy 116: “Historically, military deception has proven to be of considerable value in the attainment of national security

[59] CJCS, JP 1-02, 2000, pp. IV.

[60] Armstrong, 1998.

objectives, and a fundamental consideration in the development and implementation of military strategy and tactics. Deception has been used to enhance, exaggerate, minimize, or distort capabilities and intentions; to mask deficiencies; and to otherwise cause desired appreciations where conventional military activities and security measures were unable to achieve the desired result."[61]

5. Operational Security (OPSEC)

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations. Furthermore, OPSEC identifies those actions that can be observed by adversary intelligence systems. It can also determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. OPSEC will serve to select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.[62] OPSEC is ensuring operational data or plans aren't conveyed to an adversary.

OPSEC focuses on three key elements when involving military operations. First of all, OPSEC is concerned with denying critical information about friendly forces to the adversary. The intent is for opposing commanders, individuals, or groups to make faulty decisions based on insufficient information.[63] The second element of OPSEC is its relation to the news media. The constant pressure and presence of the news media will complicate OPSEC because

[61] DOA, 1978, pp iii.

[62] CJCS, JP 1-02, 2000 pp. VIII.

[63] CJCS, JP 3-13, 1998, pp. II-1.

news organizations offer commentary and may portray military operations incorrectly. Furthermore, the news media will be a source of information for opposition groups. Next, OPSEC can serve to delay the decision process of opposing IO targets. Through OPSEC critical information denied to an opposing IO target can be replaced or refocused to support the CCTF goal of psychological operations by identifying for attack particular adversary collection, processing, analysis, and distribution systems.[64]

OPSEC, like the other elements of IO, can support or interrupt the decision cycle of both the CCTF and the opposition commanders. As mentioned earlier, IM is performed at all levels, regardless of the extent of automation available to the CCTF. An effective IM system will provide a solid base for an effective IO plan and OPSEC will support the CCTF IO plan. The standard operating procedures associated with INFOSEC, OPSEC, and COMSEC are all anchored in an individual's thought processes. All security programs rely on the mental ability of the individual to understand the policies and always " do the right thing." They must realize the ramifications of their actions, from discussing operational information on an open telephone line to sending people's social security numbers over unclassified email.[65] The control of an individual thought process relies on the OODA decision-making loop described in Figure 4. A lack of complete OPSEC in the CCTF can disrupt the entire decision-making cycle.

[64] CJCS, JP 3-13, 1998, pp. II-2.

[65] Morthland, 2002.

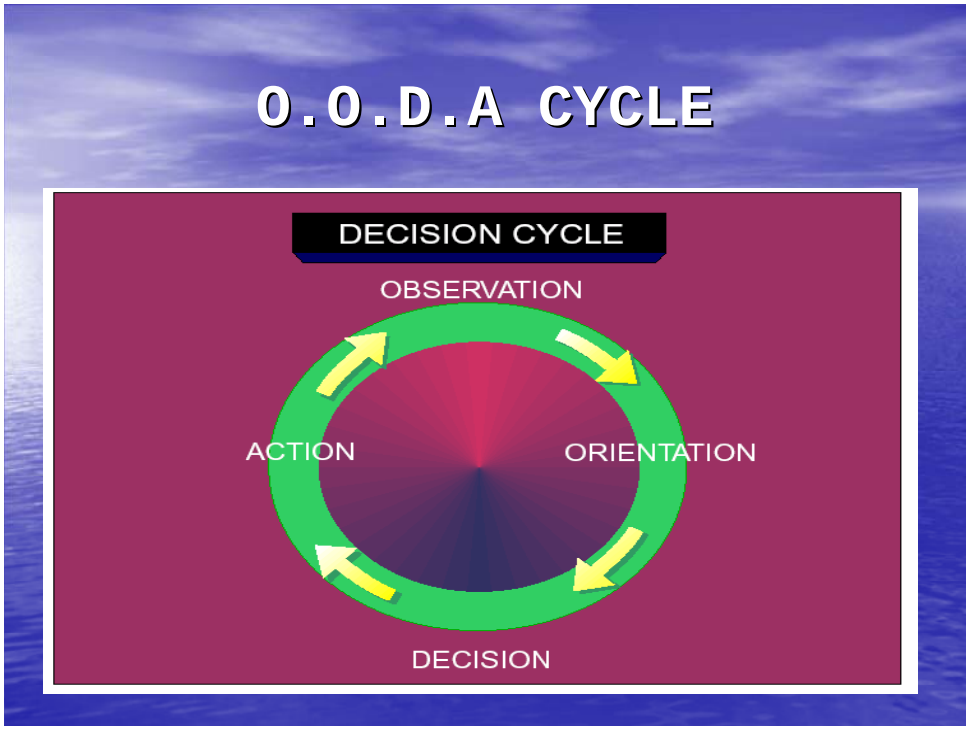

Figure 4. COL JOHN BOYD'S DECISION CYCLE.[66]

The goal of OPSEC is to protect the critical information of the CCTF. Critical Information consists of information and observables about your activities, intentions, capabilities and/or limitations that must be denied to your adversary in order to keep that adversary from gaining a technological, economic, political or military advantage. Critical information varies from organization to organization as well as from project to project.[67] According to the OPSEC Professionals Society that was established in March 1990 to further the practice of Operations Security as a profession, OPSEC is a five-step process:

(1) Identify the Critical Information: In this step, you identify which information must be protected to ensure that your adversary does not gain a

[66] MindSim Corp, 2003.

[67] OPSEC Org, 2003.

significant advantage. To determine critical information, the adversary will link critical indicators to make assumptions or uncover logical patterns that provide a route to the facts or activities that need protection.

(2) Analyze Potential Threats: In step two, you identify your adversaries, their goals, capabilities, and intentions. NOTE: The analysis of threats and the identification of critical information form a continuous cycle, where the needs and capabilities of the adversary are consistently evaluated against the critical information being considered. In other words, work back and forth between Step 1 and Step 2.

(3) Analyze Your Vulnerabilities: This third step is the heart of the OPSEC process. By now you know which information is critical to keeping your plan or project both operational and successful. You also know who is likely to want this plan or project to be derailed, as well as who is likely to want to steal it from you. You should have also identified what information would make it possible for your adversary to obtain your critical information *in time* to successfully derail or steal your project.

(4) Risk Assessment: Is a decision making step that may be considered the process of balancing vulnerability against the threat, and then deciding if the resultant risk warrants applying a countermeasure. You will need to estimate the potential effect of vulnerability on your plan or project and do a cost-benefit analysis about countermeasures.

(5) Application of Countermeasures: OPSEC Countermeasures are any actions, which deny or reduce the availability of critical information to an adversary. The most effective countermeasures are simple, straightforward, procedural adjustments that effectively eliminate or minimize the generation of indicators. Following a cost-benefit analysis, countermeasures are implemented in priority order to protect vulnerabilities that have the most significant impact on your plan or project.[68]

[68] OPSEC Org, 2003.

OPSEC violations and vulnerabilities can be prevalent in many forms. Typical vulnerabilities include: the absence of guards to secure or sensitive areas, poor or non-existent access controls, lack of software controls, and poor implementation of an OPSEC program.

The gathering of one piece of unclassified data may not indicate actual military operations or current planning. However, the accumulation of numerous pieces of unclassified critical information may indicate operations and place soldiers at risk. Lt. Mike Elliot, command OPSEC officer for USS Kitty Hawk CV-63 state, “OPSEC is protective measures we put on ourselves to restrict the flow of information that is not necessarily classified, but is sensitive in nature.” Elliot also indicated that OPSEC works under the principle that one or more pieces of unclassified material can reveal classified material. By putting together several pieces of seemingly harmless information, an enemy could damage the security of a ship and its mission. The goal of OPSEC is to avoid giving any indication of what Kitty Hawk’s intentions or missions are.[69]

6. Electronic Warfare (EW)

Electronic Warfare is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support.

[69] Beyea, 2003.

Electronic Attack (EA) is the division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).

Electronic Protection (EP) is the division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

Electronic Warfare Support (ES) is the division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. ES data can be used to produce signals intelligence, provide targeting for electronic or

destructive attack, and produce measurement and signature intelligence.[70]

7. Public Affairs (PA)

The media can be a powerful ally in disseminating truthful information regarding U.S. objectives and practices.[71] The effective use of the media is compatible with being truthful and achieving clear national security goals. But it is also clear that all too often national security goals are confused with political goals and that political fallout from successful information warfare operations can result in political backlash.[72] It must be clear to the IO cell that national security goals are not just the political goals of some faction of the MPAT. The relationship between the CCTF PAO and the IO Cell is critical.

Public affairs (PA) are public information, command information, and community relations' activities directed toward both the external and internal publics.[73] For MPAT, the external pubic is any individual or group not directly associated with the military actions being conducted in the MNF environment. The internal public is defined as individuals, groups, or organizations that are directly involved or located within the MPAT AOR. The Military actions will normally result in some type of media coverage regardless of the scope of action involved. Almost all operations will be of some interest to the general public, local and international media, and/or the committed forces

[70] CJCS, JP 1-02, 2002, pp. VI.

[71] Lacey & Bill, 2000, chap. 20.

[72] Adams, 1998, pp. 278.

[73] CJCS, JP 1-02, 2000, pp. II-2.

and their families.[74] Joint media and public affairs interactions must be considered an integral part of IO.

The bottom line facing the IO Cell with regards to PA is the connection between deception and establishment of credibility. The desire to ensure the military's survival poses a conflict for public affairs between the need to use deception practices such as collaborative deception, concealment, and omission of facts, evasion, and the need to maintain credibility with the media.[75] For example, in the summer of 1862, the Confederate Army was able to deceive the Union Army into thinking they faced a much larger force than existed. The Confederates did this in part by planting disinformation in the Richmond, Va., and newspaper and by shifting troop locations.[76] Current U.S. law and restrictions forbid deception or misleading types of military public affairs operations due to U.S. Title 10 restrictions. CNN correspondent put it best when he said, "Don't lie to me. You don't always have to tell me everything, but don't hype it either. If we think you're always hyping, we are not going to take you seriously and you won't have credibility."[77]

U.S. Public Affairs Officers (PAO) will not lie to international or local media. However, the IO Cell, the civil-military operations, and public affairs operations may be different; they should not contradict one another or the credibility of all three may be lost.[78] Although each

[74] CJCS, JP 3-61, 1997, pp. III-4.

[75] Hernandez, 2002.

[76] Hernandez, 2003.

[77] Wolf Blitzer, CNN correspondent (Public Relations Tactics, 1998, p. 18.

[78] CJCS, JP 3-61, 1997, pp. III-12.

cell will have different audiences and different informational messages, there may be an overlap of information. The de-confliction of the message is crucial. PAO are very weary when dealing with IO operators due to the legal aspects of IO operations. For MPAT operations, the mission of CCTF Public Affairs (PA) is to expedite the flow of accurate and timely information about the activities of multinational forces in the CCTF AO to the external and internal publics. News media and Public Affairs planning and coordination must be an inherent part of all CCTF planning because it is a fact accepted by every PAO in the military that most reporters are extraordinarily ignorant about the subjects they cover.[79] If properly planned and coordinated, public affairs programs can enhance and reinforce the CCTF's IO mission.[80]

[79] Adams, 1998, pp. 285.

[80] MPAT SOP, 2002, pp. C10-1.

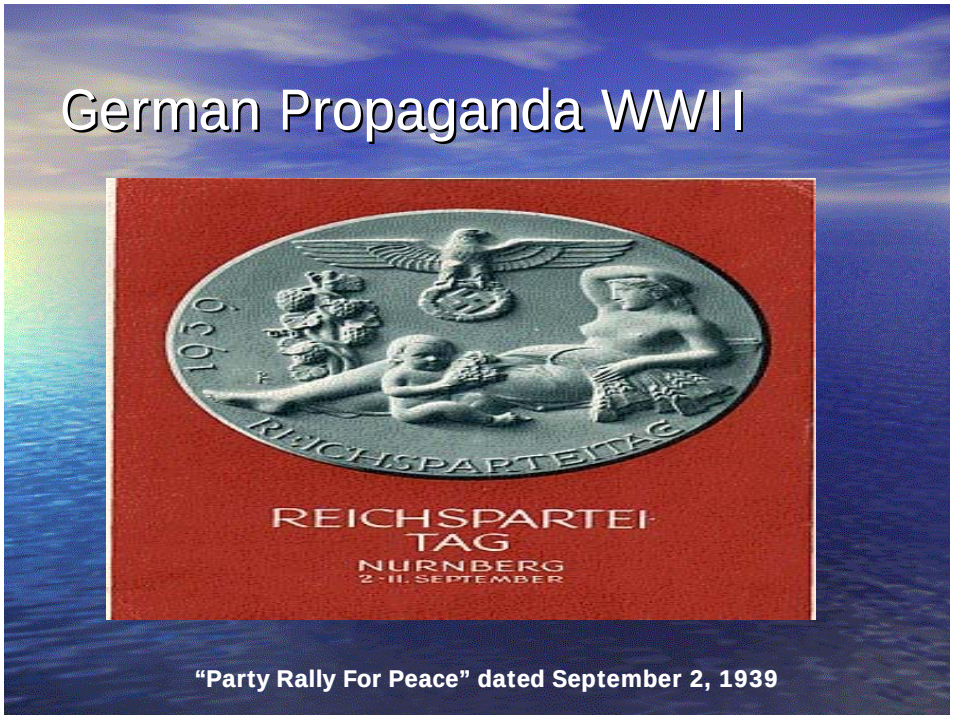

Figure 5. GERMAN POSTCARD "PARTY RALLY OF PEACE"[81]

8. Civil Military Operations (CMO)

Civil-military operations are the activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. Forces have been conducting civil-military operations for years, however only recently has

[81] This postcard was produced for the 1939 Nuremberg Party Rally, which was to be the "Party Rally of Peace." It was canceled upon the outbreak of World War II. Propaganda postcards were sent to Nazi party members.

their been an attempt to tie doctrine and action together regarding such operations.[82]

In the past, these operations were often viewed as, "that nonmilitary stuff you do after the war."[83] These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces. Civil-military operations will be discussed in greater detail in Chapter III under challenges to MNF IO.

9. Computer Network Operations (CNO)

Computer Network Operations encompass both Computer Network Defense (CND) and Attack (CNA). CND are measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. The goal of CND is to defend against an adversary's ability to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CNA operations are used to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA.

[82] Leonard, 2000, pp. 33.

[83] Leonhard, 1998, pp. 33.

Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA.

The intent of Computer Network Attack can range from total paralysis to intermittent shutdown, random data errors, wholesale theft of information, theft of services, monitoring, and the injection of false message traffic.[84] First, the IO operators or attackers will penetrate the system. The penetration phase serves to search for passwords, gain access, find unused accounts, and establish covert access to an account. The second phase of the CNA attack is to penetrate and act. This phase includes actions to gain entry, check for surveillance and gain system control. Next, the goal of attack includes search directories, acquire useful data, evidence detection, and destroy surveillance and evidence. Finally, the attacker should replace controls and logoff.[85]

Computer Network Attacks can and are likely to come from entities or groups opposing MPAT operations as well as nations states. Numerous tools are available to the IO warriors. For example, network scanners, packet sniffers, password crackers, buffer overflows, remote shutdown, domain name service hacks, web hacks, tampering, and social engineering are all widely tools available for CNA operations.[86] The coordination between the IM, IA, IO, and users of any computer system must account for the capability and criticality of the CNA threat. Table 4 summarizes the actions, objectives, and descriptions of the CNA:

---

[84] Libicki, 1996, pp. 49.

[85] Waltz, 1998, pp. 261.

[86] Dennin, 1999, pp. 209-237.

Intrusion Action	Functional Objective	Description
Access	Unauthorized access	Invalid user gains access to system
Denial	Denial of service	Disruption of message system, rendering it completely inoperable or reduced in operating capacity
Intermessage	Masquerade (spoofing)	Invalid user impersonates valid user to gain access, then misuses facility, pretends to originate message or falsely acknowledges receipt
	Message modification	Message integrity (e.g., component, address, content, labeling) is compromise while in transit
	Message replay	Valid message is repeated for purposes of exploitation
	Information leakage	Transmission monitoring to measure traffic level, traffic source destination, or content
Intramessage	Repudiation	Message system denies origin, submission, or delivery
	Security context violation	Security context is broken and message is submitted, delivered, or transferred in breach of security policy
Data Storage	Routing modification	Corruption of routing directory
	Message preplay	Delivery of a deferred message prior to authorized delivery
	Information corruption	Message integrity is compromised while in storage

Table 3. PRIMARY ACTIVE THREATS TO NETWORK MESSAGING[87]

[87] Sadeghiyan, 1992, pp. 38.

CND is a subset of computer network operations and defensive IO. The CCTF IO Cell should ensure that CND and defensive IO are not viewed as synonymous. As mentioned above, defensive IO deals with availability, integrity, authentication, confidentiality, nonrepudiation, and restoration of the entire information environment. CND deals with the technology associated with the information environment as applied to computers, weapons systems, and electronic information sharing and distribution systems. Unlike CNA, where access into the system is the key, computer network defense attempts to limit access to authenticated users. The process of authentication requires the user to verify their identity, establish access to the system, and the system to verify the user. Access controls serve only to restrict the processes that may be performed by the authenticated user attempting to gain authentication.[88]

For MPAT operations, a host of products and procedures are available to protect information systems. CCTF should ensure firewalls are present. They provide authentication, packet filtering, application filtering and state and context analysis. Other processes include encryption with the use of secret or public algorithms, digital signatures, and key management. The organization may also use vulnerability scanners, content scanners, risk analysis, tool updates, security advisory services, certification procedures, and physical security measures.[89] Table 5 summarizes the incident categories, types, and typical responses associated with CND operations.

[88] Waltz, 1998, pp. 316.

[89] Waltz, 1998, pp. 301-356.

Category	Incident Types	Typical Response
Network IW	Normal advisory	Determine own vulnerability
	Network-wide structured attack advisory	Increase alert status Tighten filters and protective measures for similar actions
External incidents	Scanning, probing	Tighten protective measures
	Intrusion attempts	Seduce scanner Initiate net trace and trap measures Selectively deny address access Terminate offending connections
	Denial of Service attacks	Selectively control service responses Attempt source identification
Internal activities	Change in trust state of detection of invalid digital signature	Change security level of system Terminate secure activities Antiviral or system diagnostic procedure
	Malicious code: installation, residence, or activation.	Terminate operations Initiate antiviral or system diagnostics
	System fault	Change security level of system Terminate secure activities Initiate system diagnostics
	Insider unauthorized access attempt	Tighten protective measures Seduce insider to monitor Initiate trace and trap measures

Table 4. INCIDENT CATEGORIES, TYPES, AND RESPONSES[90]

[90] Waltz, 1998, pp. 331.

10. Intelligence Support (IS)

Intelligence and counterintelligence requirements include current intelligence, background studies of foreign countries, and intelligence and counterintelligence estimates. Each CCTF must evaluate its assigned missions and operational areas to identify specific IO intelligence and counterintelligence needs. The thoroughness of this evaluation will determine how effectively intelligence gathering organizations and counter-intelligence support organizations and produce products. Development of IO-related intelligence and counterintelligence should be predicated on a detailed collection plan with specific collection requirements to exploit all available sources and techniques. It should include basic intelligence and country studies on foreign cultures and particular target groups as well as current intelligence on foreign group attitudes, behavior, and capabilities.

Intelligence support has two main sources. First, open sources, these can be both human and technical. The MPAT should utilize open source intelligence in any form. Sources of this intelligence include foreign radio, printed material, diplomatic reporting, radio, and the Internet. The second source of intelligence support is characterized as closed source. Closed sources can also be either human or technical. Human sources can foreign agents, diplomats, state representatives, law enforcement, defectors, and friendly third-party sources.[91] On the technical side, CNO can be supported by numerous technical sources that may be available to the MPAT. For instance, surveillance imagery, electronic signals, communications traffic, network

[91] Waltz, 1998, pp. 117.

analysis, network message interception, and computer intrusions may be available to the MPAT. Depending on the assets available in the AOR, a verity of sensors can provide detailed intelligence support to the IO Cell. Space assets, air platforms, ground platforms, and sea platforms should be considered when evaluating the IS available to the cell. Intelligence should be provided continually about specified target groups to keep IO plans and estimates current and to provide feedback to the CCTF. Proper intelligence enables clear perception and decision-making.[92] There are six basic forms of intelligence that complete the process of intelligence production and dissemination. A description of the complete process is included in Table 5 below.

[92] Waltz, 1998, pp. 219.

Phase	Description
Collection Planning	Government and military decision makers define, at a high level of information abstraction, the knowledge that is required to make policy, strategy, or operational decisions.
Collection	Following the plan, human and technical sources of data are tasked to perform the collection. These sources include open and/or closed human or technical.
Processing	The collected data is indexed and organized in an information base, and progress on meeting the requirements of the collection plan is monitored. As a result of collection, this organization data may adjust the plan on the basis of received date.
Analysis	The organization information base processed using deductive inference techniques that fuse all source date in an attempt to answer the requester's questions.
Production	Intelligence may be produced in the format of dynamic visualizations on a war fighter's weapons system or in formal reports to policy makers.
Application	The intelligence product is disseminated to the user, providing answers to queries and estimates of accuracy of the product deliver.

Table 5. INTELLIGENCE CYCLE[93]

F. SUMMARY

The IO cell must focus on precision engagement and full dimensional defense to be successful. All the elements of IO can exploit the sensors, delivery systems, and effects during MNF operations. They can protect the personnel and other assets required to decisively execute assigned tasks. For IO, information is the medium, and

[93] Waltz, 1998, pp. 113.

information exploitation is an opponent’s resource to be targeted to achieve information dominance.[94]

[94] Adams, 1998, pp. 17.

III. UNIQUE ASPECTS OF CONDUCTING MNF IO

…Those horrible pictures of newly elected Panamanian Vice President Ford, covered head to toe with blood, beaten mercilessly.[95]

-President G.H.W. Bush, 1989

A. INTRODUCTION

The unique organizational structure of the MNF MPAT organization with a multitude of many planners from different nations coming together during a time of crises offers the IO planner and operator unique challenges. During MPAT operations there are always multiple chains of command. Each nation's forces fall under their national chain of command and the CCTF multinational chain of command. The National Command is never relinquished to the multinational chain of command. The Multinational Command will usually take the form of control and coordination within the CCTF chain of command. Each nation furnishing forces to the CCTF establishes a National Command Element (NCE) within the CCTF command. Normally this person is the senior officer in the CCTF for a given nation. This establishes the national command link back to respective nations' military and political authorities. The specific officer assigned as commander of this national command element may also be dual-hatted with other CCTF command and staff responsibilities.

Once the C2 organization is agreed upon by the Lead Nation, the level of support that each participating nation contributes will drive the MNF operation and eventually the associated IO actions taken within that theater.

---

[95] President George Bush addressing the Nation, describing the current events in Panama and his decision to use military force, 1989.

There are four defined levels of MPAT support that the IO planner must consider. First is the idea of “General Support”. General support is given to the supported force as a whole rather than to a particular subdivision thereof. The second theory of support is “Mutual Support” which is support which units render each other against an adversary because of their assigned tasks, their position relative to each other and to the adversary, and their inherent capabilities. Third, “Direct Support” is support of a mission requiring a designated force to support another specific force. And finally, “Close Support” is action of the supporting force against targets or objectives that are sufficiently near the supported force to require detailed integration or coordination of the supporting action with the fire, movement or other actions of the supported force. The IO SOP assumes that the type of supported called for by the Lead Nation is clear and the IO Cell fully understands the support required. Varying degrees of support may be required at the discretion of the Lead Nation Commander or CCTF Commander.

The ability of the Lead Nation and the participating Nations to clearly define strategies and objectives for the IO Cell will offer additional challenges to IO planners. Challenges will include, but are not be limited to military operations, social interactions, and technology limitations. These challenges within operations will be driven by the nature and level of support required and the command relationships constructed prior to or during MOOTW/ SCC operations.

Figure 6. MPAT C2[96]

B. CHALLENGES

A multitude of challenges face the MPAT organization and the application of IO in the MNF environment. The following planning factors may have significant impact on unity of effort and effectiveness of CCTF planning and operations. These need to be fully addressed and acknowledged in the planning process. Though IO can be related to all of the addressed challenges below, technical agreements and the advances in information and network technologies (number 10 & 11 below) are the focus of this thesis. They offer the most unique challenges facing IO Cell operators in the MNF environment. Challenges include, but are not limited too:

96 MPAT SOP, 2002.

(1) Differences in strategic national interests, objectives and policies.

(2) Availability of forces.

(3) Availability of strategic lift assets to deploy forces and equipment from national bases to the CCTF area of operation.

(4) Access to airfields and ports adjacent to the CCTF Area of Operation.

(5) Restrictions on movement of forces through sovereign territories, waters and airspace of non-participating countries.

(6) Agreed-upon coalition Rules of Engagement (ROE) and procedures for amending them

(7) Some degree of agreed-upon SOPs for the CCTF HQ and its subordinate force components

(8) Status of Forces Agreements (SOFA) / Visiting Forces Agreements (VFA) among MNF participating nations and the host nation(s) and affected nation(s)

(9) Command, control, communications, computers, and intelligence (C4I) systems interoperability and connectivity, plus frequency spectrum management and communication satellite channel availability.

(10) Technical Agreements (TA) are especially critical for logistics coordination with MNF participants and the host nation. While logistics support of MNF units is a national responsibility, existing acquisition and cross servicing and implementing arrangements should be used wherever possible. This will simplify support of deployed forces and reduce duplication of support requirements in the CCTF Area of Operations. Shared support for basic logistics functions of movement, basic sustainment (water, base supplies, etc.), and infrastructure support (port operations, rail, highway, local security) should be pursued to the maximum extent possible.

(11) Advances in information and network technologies (Internet, cryptology and information assurance

> technologies, communication satellite, off-the-shelf equipment, and technologies, etc.) should be built upon in partnership venues such as the MPAT program and other venues of dialogue, planning, and coordination.[97]

For the IO SOP the challenges were broken down into three distinct challenges: military operations, social interactions, and technology limitations.

1. Military Operations

Multinational military operations may be conducted during periods of both war and military operations other than war (MOOTW). Each multinational operation is unique, and key considerations involved in planning and conducting multinational operations vary with the international situation, perspectives, motives, and values of the organization's members.[98] Military operations with regards to IO focus on the interactions and limitations of operations when a military action or the carrying out of a strategic, tactical, service, training, or administrative military mission; the process of carrying on combat, including movement, supply, attack, defense, and maneuvers needed to gain the objectives of any battle or campaign.

[97] MPAT SOP, 2002, pp. v.

[98] CJCS, JP 3-16, 2000, pp. I-3.

Figure 6. MILITARY CAPABILITIES OF NATIONS[99]

The first challenge of the MNF IO planner is the actual interactions of members of the IO Cell. All MNF members should be represented in the IO cell in positions to contribute, when possible, to each of the elements of IO.[100] However, the levels of IO experience and understanding will differ greatly. For the cell to operate effectively, the unique talents of its members should be openly discussed as earlier as possible during operations. IO military operations will encompass a host of support from intelligence support to public affairs. The members in the cell may be able to offer indirect support in one of these roles.

The second challenge of IO in the MNF environment will be Operational Security (OPSEC). OPSEC security denies adversaries information regarding intentions, capabilities,

[99] CJCS, JP 3-16, 2000.

[100] CJCS, JP 3-16, 2000.

and plans by providing functional and physical protection of people, facilities, and physical infrastructure components.[101] For OPSEC to be effective, the sources of leaks and potential vulnerabilities must be identified and tracked. Furthermore, a key element to OPSEC is the “need to know” criteria. The very nature of effective IO is the ability for it to be covert. All members of the planning staff may require different levels of access to operate effectively in the MNF IO environment. The key will be for the IO Cell Chief to decide what operations and at what level will members be allowed to review and input into IO plans.

A third challenge to military operations will be the prioritization of actions. All members of the IO Cell must focus on the interests at hand. An interest taxonomy chart is a useful tool for any planner. For instance, each IO action can be seen as a separate task. Each task has specific characteristics such as importance or duration to the overall IO plan. The planner then decides at what level of importance: is the IO action a primary or a secondary concern to the CCTF. Finally, the weight of the decision being made should be examined. For instance, the IO Annex should include a matrix that may be utilized to focus effort. Table 6 is an example of such a matrix.

[101] Waltz, 1999, pp. 222.

ASPECT OF INTEREST	LEVEL OF INTEREST	WEIGHT OF IMPACT	EXAMPLES
Importance	Primary *Secondary*	Core Strategic *Significant Value*	Deter terrorist actions *Expose terrorist Leadership*
Duration	Primary *Secondary*	Permanent *Uncertain*	Ensure flow of information *Support opposition activities*
Focus	Primary *Secondary*	Specific *General*	Deny terrorist communications *Destroy terrorist camps*
Compatibility	Primary *Secondary*	Complementary *Conflicting*	Support military operations *Unable to provide forces*
Influence	Primary *Secondary*	Enduring *Temporary*	Combat Terrorist Leadership *Commit military forces*

Table 6. INTEREST TAXONOMY[102]

The IO cell will have to deal with from the multinational information release criteria when planning and conducting MNF IO. For the U.S., the policy is that the appropriate U.S. geographic combatant commander should issue clearly stated guidelines for the release of classified U.S. information to the MNF, based on existing policy directives and any applicable approved exceptions to national disclosure policy. These guidelines should be issued to U.S. participants only and should be specific enough to allow implementation down to the tactical level. The subordinate JFC may undertake planning and execution of independent IO in support of multinational objectives.[103] The non-US members of the coalition will face the same challenges when dealing with coalition-classified

[102] Liotta, 2000, pp. 129.

[103] CJCS, JP 3-16, 2000, pp. IV-13.

information. For IO, many of the current tools and delivery methods are classified and carry restrictions on foreign classifications. These limitations on the release of classified material may hinder successful IO operations.

Finally, the MNF IO cell will face disagreements when dealing with IO targets and related Coalition Rules of Engagement (CROE). As mentioned in Chapter II, IO targets can vary greatly. For certain members of the MNF, the targeting of civilian infrastructure is appropriate if it meets military objectives. However, not all nations will agree upon the CROE and targets available for IO attack. IO planners must clearly understand the CROE and how they apply to IO. As directed in the MPAT SOP, "The Supported Strategic Commander should publish CROE at the earliest possible date after approval by the Lead Nation, in consultation with supporting nations' and Supporting Strategic Commanders. The Supported Strategic Commander will make the widest possible distribution of the CROE to assist in overall CCTF planning and refinement as required."[104] Attacking the wrong target and applying the wrong CROE can bring into jeopardy the entire operational plan, not just the IO operation.

To minimize disagreements in the CROE with regards to IO CROE, they must presented to higher authority with-in the CCTF via all chains-of-command including the host nation and representative commanders from participating nations. Each CCTF is directed to create a targeting board with selected representatives from each independent cell including the IO cell. Included at these targeting boards are legal representatives from participating nations if

[104] MPAT SOP, 2002, pp. C3-F1.

available. Legal issues and CROE disagreements must be presented in this forum early in the planning cycle to avoid unforeseen consequences of illegal or immoral actions that may jeopardize the entire IO plan.

2. Social Interactions

Social interaction challenges will focus on civil-military operations or group of planned activities in support of military operations that enhance the relationship between the military forces and civilian authorities and population and which promote the development of favorable emotions, attitudes, or behavior in neutral, friendly, or hostile groups. Civil-military operations have usually focused on the strategic level of interaction between highest political authorities and senior military leaders. Recently the focus has expanded to include the nature of relationships between society and the military institutions the society supports. The dynamics of civil military relations also can include the nature of relationships between soldiers and sailors on weekend passes in the local town, whether at home or abroad.[105] It includes the relationship between the CCTF, the host nation and the local authority of the town, city, or AOR.

The social interaction issues that the IO Cell will face are three-fold. The problem that may be encountered falls in the realm of the limitation of experience between civilian and military decision makers. For example, it has been hypothesized that military decision makers are better prepared to deal with current and future military decisions than are their civilian counterparts. Second, neither the civilian leadership, nor the military services have a common vision of the future. Third, both parties to the

[105] David, 1996, pp. 5.

relationship, as well as the general public, are changing their ideas of what "correct" or "good" civil-military relations should be in today's environment.[106] In the ideal situation, the military acts as an agent of the civilian leadership. The solution to the problem is to generate civilian consensus.[107] For the CCTF IO Cell and the CCTF a consensus of action regarding the strategic, tactical, and operational goals of the IO plan are crucial to maintain solid civil-military agreement. If the CCTF can present consensus, the civilian leadership may disagree, but it will have minimal leeway to alter the IO course of action.

3. Technology Limitations

The greatest challenge to the IO cell will be technology. Technology limitations will encompass interoperability or the ability of systems, units or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.[108] Technological limitations will be apparent in weapons, transportation, information, and support both logistical and personnel. For the IO Cell, the focus will remain with the limitations associated with information and its control.

The United States outspends the West Europeans in the areas of defense modernization and R&D by a ratio of roughly 2:1.[109] Thus, it is probable that technological limitations will be handled with policy "workarounds" rather than through technological "fixes."[110] The key to

[106] Snider, 1996, pp. 8.

[107] Avent, 1996, pp. 20.

[108] CJCS, JP 3-16, 2000, pp. GL-6.

[109] Nichiporuk, 2000, pp. 25.

[110] Nichiporuk, 2000, pp. 27.

technological limitations with information is to standardize in and or to achieve interoperability, compatibility, interchangeability, and commonality. The MITRE CORPORATION offered one solution; they have created a model to help planners identify shortcomings with regards to C4I technologies encountered in the MNF. In their model, there are five level of interoperability:

(1) Level 0 is the isolated or manual level.
(2) Level 1 deals with a connected or peer-to-peer architecture.
(3) Level 2 is Functional or distributed.
(4) Level 3 is the Domain or integrated.
(5) Level 4 is the Enterprise of universal.

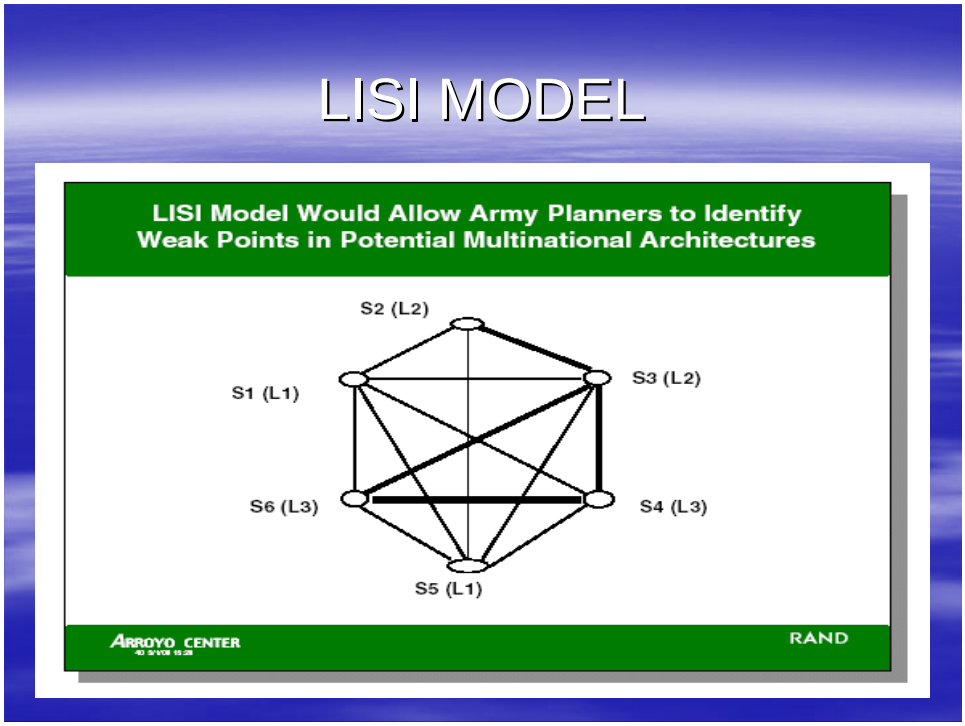

Figure 7. LISI MODEL[111]

Figure 7 provides a notional portrayal of what a LISI compatibility map might look like for a given U.S. ally or partner. If we assume that nodes S3–S6 are U.S. systems and S1–S2 are the ally's systems, this map portrays the

[111] MITRE Corporation, 2001.

compatibility levels of each system-to-system interaction. The “L numbers” in parentheses denote the compatibility level of each system, and the overall level of compatibility between two systems is the lower of the two numbers. Thus, the level of compatibility between an L1 and an L2 system would be L1. The darker the line on the map above, the higher the level of compatibility.[112] The above model offers a simple way to decide what technological limitations of the force may be present. The use of the LISI Model will offer the planner the ability to find compromises and work around as required. They offer the ability of future MPAT planners to identify and invest was required to help avoid future problems of the MNF.

C. LIMITATIONS OF IO POLICIES

The limitations of the IO plan within the CCTF will be driven by three operational factors or elements of war fighting: time, space, force. Additionally, the interaction of legal aspects of IO and risk of conducting IO, will add additional limitations to the overall IO plan. A common understanding of each factor is required to ensure the IO Cell operates successfully when faced with the limitations and constraints of each. It is not easy to predict which factor or combination of factors will add the most limiting weight to an operation, however a basic understanding of the influencing factors of each element is required to minimize problems that might arise.

If the operational factors are brought into balance, it will allow the CCTF more freedom to act and act decisively. However, one or more of these factors may limit the commander’s ability to act. One may require more

[112] Nichiporuk, 2000, pp. 28.

troops, more time to accomplish the mission, or more latitude while engaging the enemy. Information Operations also suffers from these limitations because there is only a finite amount of each factor. Furthermore, the IO cell may not be able to control or influence one or more of these factors.

1. Time

During military actions, all forces will face some restraints when dealing with time. Few operations have an unlimited timeline to accomplish a mission. Leadership, diplomatic, media, and local pressure can force an end to an operation. Furthermore, many operations fail to maintain support because the correlation between time and accomplishment of the mission is not linear.

Time has numerous driving forces. The IO Cell must consider them all. Time considerations include preparation, information handling, intelligence, the decision cycle, warning, reaction, counteraction, and C2. One or more of these factors will drive operational planning within the MPAT. Time is the most important element with regards to operational factors. The factor time is defined as with the time that it takes the commander to execute one cycle through an OODA loop.[113] This time is related to the duration of the sub-activities within the OODA loop, including the time to observe/sense, orient/process and compare, decide, and act. Time assets and never be recovered; space and force may be corrected. Table 5 summarizes the factors affecting time:

[113] Mclure, 2000, pp. 21.

TIME CONSIDERATIONS	NOTE:
Preparation	How long does it take to create the IO plan?
	How long to get IO forces in the AOR?
Information Gathering	How long does it take me to gather process and disseminate information?
Decision Cycle	How long does it take a decision to be made once the information is gathered?
Timing	When should I do it?
Warning	How much warning time do I have?
Reaction	How long does it take him or me to react to an IO task?
C2	How quickly does the C2 organization work?
Between Operations	How much time do I have between operations?
Gaining and Losing	When and where will I gain or loss time?
Duration	Will my actions prolong the operation?

Table 7. TIME LIMITATIONS[114]

2. Space

Space or battlespace elements will offer vary unique challenges for the IO Cell. Space will include shape, geography, terrain, and physical elements of the theater, military organization, distances, physical characteristics, and geostrategic position. Advances in technology, information age media reporting, and the compression of time-space relationships contribute to the growing interrelationships between time, space, and force. CCTF's should ensure that their joint operations are integrated and synchronized in time, space, and purpose with the actions of other military forces (multinational

[114] Mclure, 2000, pp. 28.

operations).[115] To achieve this, synchronization must take place in the physical domain (potentially in the information domain as well, in the case of information operations) to create effects in the battlespace.[116]

3. Force

The next factor affecting any IO operations is the question of force. The consideration affecting the force and its structure are numerous. The CCTF and the IO Cell must decide on the more important ones, a risk-based calculation is required. Force considerations include: size, type, mix, flexibility, combat power, transportation, organization, reserves, logistics, mobility, weapons, and equipment. Any one of these elements may be the key to successful operations. Other operational factors of force will include public support, the will to fight, training, leadership, moral, soundness of doctrine, and the overall combat readiness of troops.

For the IO Cell the organization of the cell is one of the most crucial aspects. Organization and structure of the cell will include numerous operators and managers all with different goals. For instance, the IO Cell should include a PA representative and an Intel representative, each will have different directives and goals. How well the IO Cell relates to individual members inside and outside the cell, may ultimately affect the success or failure of the IO operation.

4. Legal

The growth in IO related technology and capabilities and associated legal issues makes it critical for

[115] CJCS, JP 3-0, 2001, pp. II-6.

[116] David, 1996, pp. 73.

commanders at all levels of command to involve their staff judge advocates in development of IO policy and conduct of IO.[117] The guidance given to the MPAT is that selected International Agreements, Law of Armed Conflict, Treaties Governing Land Warfare, The Law of Land Warfare, and other applicable armed conflict legal guidelines and documents will govern CCTF forces in the conduct of operations. Commanders are responsible to ensure persons subject to their authority are aware of the limitations and standards imposed by international law and that personnel adhere to such standards.[118] However, this guidance is limited and a further discussion of the legal limitations of IO is required.

IO can be an offensive weapon thus the Laws of Armed Conflict and the Principles of War apply to almost all IO operations. IO will face all challenges of any military action in the courts and in the public. Specifically, IO issues may involve of the Law of Neutrality, Law of War, and Perfidy versus Lawful Deception, Law Enforcement, and Communications Monitoring. The emerging discipline of IO synthesizes laws and policies related to intelligence collection and oversight, space law, computer security, psychological operations, mission planning, law of armed conflict targeting constraints, information security and exploitation, and search and seizure guidelines. There are many areas where current laws contain gaps, which can frustrate commanders who seek

[117] CJCS, JP 3-16, 2000, pp. II-8.

[118] MPAT SOP, 2002, pp. C9-5.

crystal clear answers for important operation issues.[119] Table 5 summarizes some of the critical issuing facing IO.

[119] Lacey, et al., 2000, chap. 20.

LAW/ISSUE	DESCRIPTION
Law of Neutrality	All acts of hostility in neutral territory, including neutral lands, waters, and airspace are prohibited. Using wires or digital cables of a networked associated with a neutral party, as a conduit for IO would jeopardize that State's neutrality.
Law of War	The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.
	The right of belligerents to adopt means of injuring the enemy is not unlimited.
	Those who plan or decide upon attack shall take all feasible precautions in the choice of means and methods of attack with a view of avoiding, and in any event, to minimizing, incidental loss of civilian life, injury to civilians, and damage to civilian targets.
	The collateral damage may not be excessive in relation to the direct and concrete military obtained through the destruction of the intended target.
Perfidy	Prohibits belligerents from killing, injuring, or capturing and adversary by perfidy.
Law Enforcement	U.S. military does not engage in law enforcement.
COMSEC	COMSEC monitoring IO campaign is permitted.
	Information Systems Security Monitoring will be conducted only in support of security objectives.
	Information Systems Security Monitoring will not be performed to support law enforcement or criminal or counterintelligence investigations.

Table 8. IO AND LAW[120]

[120] Lacey, et al., 2000.

Problems when operating in a multinational force structure may be complicated by varying national obligations derived from international agreements. Other coalition members may not be parties to treaties that bind the United States, or treaties to which the United States is not a party may bind them. U.S. forces will comply with the Law of War during military operations involving armed conflict, no matter how the conflict may be characterized under international law, and will comply with its principles and spirit during all other operations. Furthermore, U.S. forces assigned to the operational control (OPCON) or tactical control (TACON) of a multinational force will follow the ROE of the multinational force for mission accomplishment if authorized by the National Command Authority (NCA).[121] IO Cell operators must familiarize themselves with the Status of Forces Agreements and must ensure all IO actions are cleared through legal representatives.

5. Risk

Risk will always be an integral part of any information operation; it is unavoidable. Those unable to understand the dangers inherent in employing troops are equally unable to understand the advantages way of doing so.[122] The tradeoff between benefits of information access and the consequences of attacks by imposing threats requires a management of the level of risk imposed upon the system.[123] Risk in its most basic form can be described by the equation:

[121] CJCS 3121.01A, 2000, pp. A-1.

[122] Tzu, 1975, pp. 73.

[123] Waltz, 1998, pp. 156.

Risk = [Threat x Vulnerabilities/ Protection] x Impact

The IO Annex has gone beyond this simple equation to help planners assess the risk involved in IO. For instance, utilizing a combination of author created and standard U.S. IO handbook created charts in the IO Annex, the operator will be able to assign numbers to risk. For example, when dealing with the “Opposition’s conduct of the Activity”, by assigning a number to each and calculating the total, the risk can be determined. The IO Annex provides an IO task selection tool. Each included form drives the planner to calculate the best and most effective IO tool to complete an assigned mission. Forms 1 through 7 establish the specific and implied tasks, Forms 8 through 22 refine the task and assign IO tools to complete the task. For example, the Commander’s assigned task is: *To neutralize Iraqi guerillas ability to coordinate attacks and to expose resistance members.* Examples of Form 8 and 9 below explain how activity and benefit are calculated to help aid the planner.

(1) FORM 8: Opposition Activities will be affected.
   a. IO objective: “The U.S. will diminish the guerillas’ ability to communicate to resistance members”
   b. Opposition Activities that will be affected:
      i. Lines of Communications,
      ii. Recruitment opportunities,
      iii. Planning and organization of attacks,
      iv. Administration activities,
      v. The ability to communicate critical information to operators and planners of attacks.

(2) FORM 9: Identify the Functions that most contribute to the Opposition's conduct of the Activity.

	Contribution (.33)			Impact (.33)			Uniqueness (.33)			Total
Enemy Function High (.8) Med (.5) Low (.2)	Role	Value	Total	Econ	Mission	Total	Redundancy	Recoverability	Total	
Target Civilians	.5	.5	.33	.2	.5	.231	.2	.5	.231	.792
Engage in CNO	.8	.5	.429	.5	.8	.429	.5	.8	.429	1.287
Increased recruiting	.2	.5	.231	.8	.2	.333	.2	.5	.231	.777

Table 9. OPPOSITION'S CONDUCT OF THE ACTIVITY[124]

Additional charts are used throughout the SOP. Charts are provided for evaluating tasks, evaluate and targets associated to identify the ones most critical to the success, and identifying IO assets. Each chart and the total calculated by operator input will produce calculations required by the IO Cell to help assess the risk of any IO offensive or defensive action when selecting IO tasks. Additional calculations can also be found in the IO Annex. For example, Figure 8 "FORM 20: COST/BENEFIT/RISK of IO Asset" can be utilized to calculate enemy COA against MPAT IO actions. Each possible COA has separate calculations complied to add the planners. The risk calculations can be compared to the cost of the action and the benefits of the action. These calculations can be completed for N number of assets. Continuing with the

[124] CJCSM 3122.03a

previous example, FORM 19 and 20 help streamline the IO task being reviewed to meet mission objectives by calculating risk. For instance:

FORM 19: Identify the IO Asset.

(1) CNO

a. Apportioned = YES
b. Assigned = YES
c. Allocated = YES
d. Deployed = YES
e. In-commission (not battle-damaged or destroyed) = YES
f. Availability = HIGH (.8),
g. Duration (.2) = MED (.5),
h. Delivery Error (.2) = LOW (.2),
i. Probability of Effect (.2) = MED (.5),
j. Asset Reliability (.2) = MED (.5)

(2) PHYSICAL DESTRUCTION

a. Apportioned = YES,
b. Assigned = YES,
c. Allocated = YES,
d. Deployed = YES,
e. In-commission (not battle-damaged or destroyed) = YES
f. Availability = MED (.5),
g. Duration (.2) = MED (.5),
h. Delivery Error (.2) = LOW (.2),
i. Probability of Effect (.2) = LOW (.2),
j. Asset Reliability (.2) = MED (.5)

FORM 20: COST/BENEFIT/RISK of CNO AND PHYSICAL DESTRUCTION

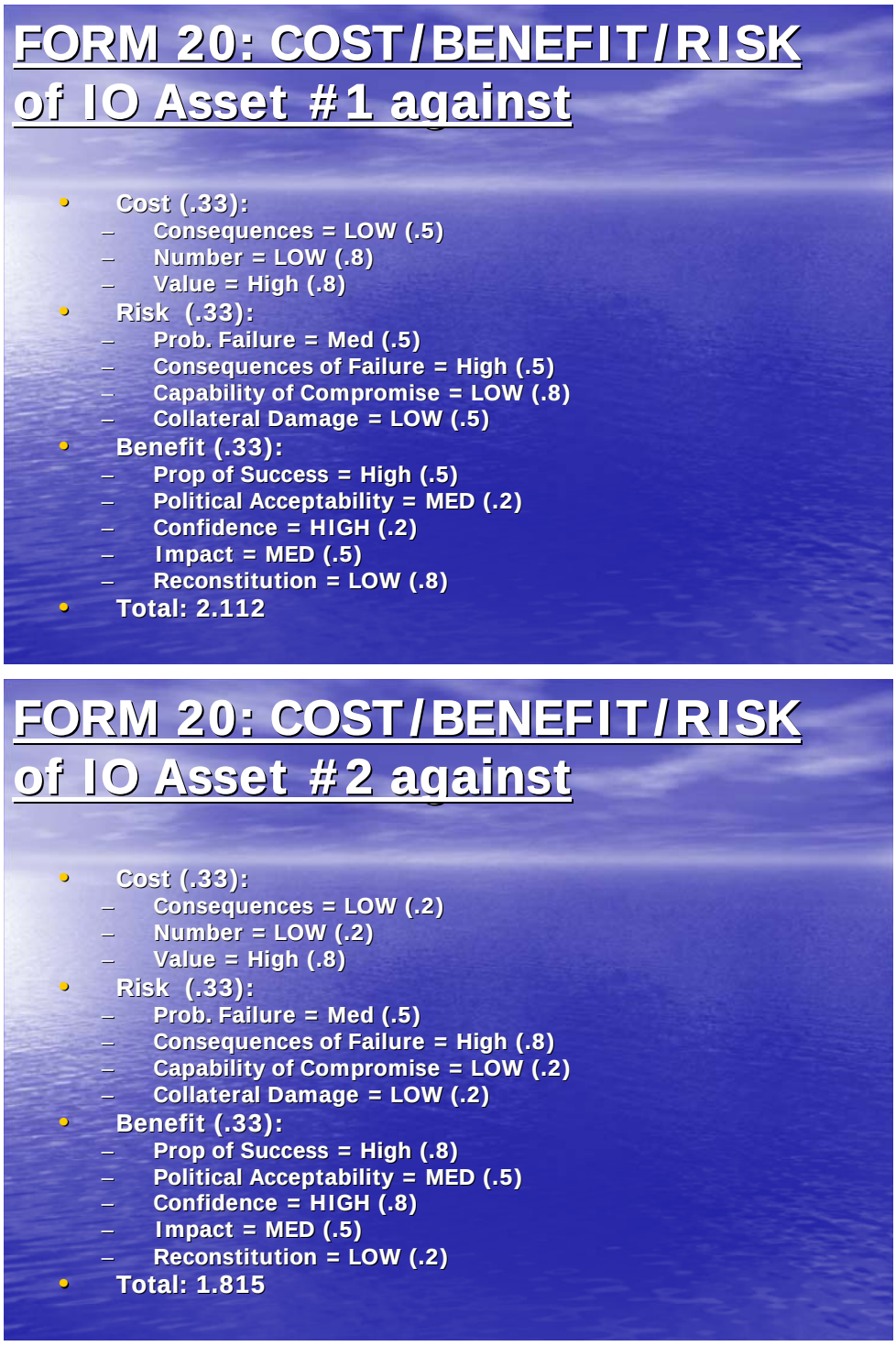

Figure 8. COST/ BENEFIT/ RISK CALCULATION

From the Form 19 and 20 above, the calculations indicate that the overall cost vice risk and expected benefit indicate that against our example task "To

neutralize Iraqi guerillas ability to coordinate attacks and to expose resistance members", the option of CNO is more viable given in theater assets. These simple calculations offer the planners the ability to present to commanders a calculation based assessment of each IO task. The cost of completing such calculations is limited by the scope the planner is willing to endure per IO task and the time allotted for planning each task and completing the calculations.

E. SUMMARY

All information warriors, staffs, and coalitions are going to encounter challenges, limitations, and risk when conducting IO in the CCTF. Military interactions, social disagreements, technological limitations, and operational factors of time, space, and force will cause the greatest and most unforeseen problems. These problems can be minimized with constant synchronization of plans and adjustments made prior to and during the execution phases of IO. IO deals with the control, manipulation, and the flow of information within and outside the AOR. However, within the CCTF and the IO cell, information and discussion must flow freely. All members, regardless of their associated limitations, must have input into the IO plans and operations because the assignment of forces and missions in ad hoc coalitions must reflect the unique capabilities of each partner.[125]

[125] Pudas, 1994, pp. 42.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE REVIEW

A. INTRODUCTION

This case study is presented because it case unique lessons learned regarding an inadequate focus on IO. The case serves to explore how IO was used during the conflict to meet strategic and operational ends. Specifically, the study will focus on propaganda, deception, and civil-military operations as used in Rwanda. It is an examination of possible themes, IO targets or sources that a group or state may attempt to utilize during MOOTW/SCC.

Rwanda was chosen because it illustrates, even given the limitations of technology are within the region; the other aspects of IO including the use of psychological and civil military are still relevant. It also offers insight into the complexity of processes and procedures, associated with the deployment of multi-national forces and the consequences of the international community failing to act effectively within the information battlespace.

B. RWANDA

1. Background

In the summer months of 1994, the African nation of Rwanda was plunged into civil war, ethnic cleansing, and massive acts of genocide. It is estimate that 1 million Tutsi and politically moderate Hutu men, women, and children were killed or tortured based on their ethnic and political backgrounds.[126] In October of 1990, soldiers led by Major General Fred Gisa Rwigyema separated from the Uganda National Republican Army and attacked Rwanda. The government of Rwanda, led by President Habyarimana, fought

[126] Keane, 1995, pp. 10.

back for the next four years as the international community watched. In July of 1992, negotiations began on the Arusha Peace Accords between the warring factions. By August 1993, the accords and the signings were completed. However, power struggles continued between the two sides throughout the year. As violence increased, the country began to tear itself apart. And finally in April of 1994, the genocide began and was fueled by radio addresses, newspaper articles, and political speeches. Major events that led to months of genocide in Rwanda were:

(1) 1989: The coffee price collapses, causing severe economic hardship in Rwanda.

(2) 1990, July: Under pressure from western aid donors President Habyarimana concedes the principle of multi-party democracy.

(3) 1990, October: Guerrillas of the recently formed Rwandan Patriotic Front (RPF) invade Rwanda from Uganda. After fierce fighting in which French and Zairean troops are called in to assist the government, a ceasefire is signed on 29 March 1991.

(4) 1990/91: The Rwandan army begins to train and arm civilian militias known as the Interahamwe. For the next three years Habyarimana stalls in the establishment of a genuine multi-party system with power sharing. Throughout this period thousands of Tutsis are killed in separate massacres around the country. Opposition politicians and newspapers are persecuted.

(5) November, 1992: Prominent Hut activist Dr Leon Mugusera appeals to Hutus to send the Tutsis ‘back to Ethiopia’ via the rivers.

(6) February 1993: The RPF launches a fresh offensive. The guerrillas reach the outskirts of Kigali and French forces are again called in to help the government side. Fighting continues for several months.

(7) August 1993: At Arusha in Tanzania, following months of negotiations, Habyarimana agrees to power sharing with Hutu opposition and the RPF. 2,500 UN troops are deployed in Kigali to oversee the implementation of the accord.

(8) September 1993- March 1994. President Habyarimana stalls on setting-up of power-sharing government. Extremist radio station, Radio Mille Collines, begins broadcasting exhortations to attack Tutsi. Human rights groups warn the international community of impending calamity.

(9) March 1994: Many Rwandan human rights activists evacuate their families from Kigali, believing massacres are imminent.

(10) 6 April 1994: President Habyarimana and the president of Burundi, Cyprien Ntaryamira, are killed as their plane is shot down while landing at Kigali Airport.

(11) 7 April 1994: The Rwandan armies' forces and the Interahamwe set up roadblocks and go from house to house killing Tutsi and moderate Hutu politicians. Thousands die on the first day. UN forces stand by while the slaughter goes on. They are forbidden to intervene because their mandate states to monitor the situation.

(12) 8 April 1994: The RPF launches a major offensive to end the genocide and rescue 600 of its troops surrounded in Kigali. The troops had been based in the city as part of the Arusha accords.

(13) 21 April 1994: The UN cuts the level of its forces from 2,500 to 250 following the murder of ten Belgian soldiers assigned to guard the moderate Hutu prime minister. He is killed and the Belgians are disarmed, tortured, shot and hacked to death. They had been told not to resist violence by the UN force commander, as it would have breached their mandate.

(14) 30 April 1994: The UN Security Council spends eight hours discussing the crises. The resolution omits the word "genocide". If the term had been

used, the UN would have been legally obligated to act based on their current mandate.

(15) 17 May 1994: As the slaughter of the Tutsis continues the UN finally agrees to send 6,800 troops and policemen to Rwanda with powers to defend civilians. The deployment of troops is delayed because of arguments over who will pay the bill and provide the equipment. The United States argues with the UN over the cost of providing heavy armored vehicles for the peacekeeping force.

(16) 22 June 1994: With still no sign of UN deployment; the Security Council authorizes the deployment of French forces in southwest Rwanda. They created a safe area in territory controlled by the government. Killings of Tutsis continue in the safe area, although the French protects some civilians. The United States government eventually uses the word ‘genocide’.

(17) July 1994: The final defeat of the Rwandan army. The government flees to Zaire, followed by a human tide of refugees. The French end their mission and are replaced by Ethiopian UN troops.

According to the current government of Rwanda, “The 1994 genocide was a carefully planned and executed exercise to annihilate Rwanda's Tutsi population and Hutus who did not agree with the prevailing extremist politics of the Habyarimana regime. One million lives were lost in only one hundred days. It is the fastest and most vicious genocide yet recorded in human history.”[127] Currently, a policy of decentralization has been initiated to involve people in grassroots communities in decision-making. This will enhance their participation in activities to transform their poor conditions. However, current indications are that Tutsi, Hutu, and other conflicting ethnic groups,

[127] Official Website of the Government of Rwanda, http:// www.rwanda1.com/government/rwandalaunchie. dated 22 Oct 2004.

associated political rebels, armed gangs, and various government forces continue fighting in the Great Lakes region, transcending the boundaries of Burundi, Democratic Republic of the Congo, Rwanda, and Uganda. Government leaders pledge to end conflicts, but localized violence continues despite UN peacekeeping efforts.[128]

2. IO in Rwanda

Rwanda had only limited sources of information operations assets available during the crises. First, there were two AM radio stations, one FM station based in Kigali (with several repeaters), one Indian Ocean INTELSAT, one SYMPHONIE satellite, and limited newspapers. However, even though it is estimated that 66 percent of Rwandans are literate, the written word and the message was often translated into graphic and violent cartoons.[129] Even with high literacy rates present throughout the region, leaders of the genocide believed their actions would be understood more clearly with graphic and violent cartoons that could be easily circulated to the most remote regions of the country. Graphic and violent cartoons would help incite further violence. Furthermore, the country lacks computers and televisions. This lack of technology required the warring factions to turn to the only source of information dissemination available, the radio.

128 CIA Fact Book, 2003.

129 Des Forges, 1999, pp. 67.

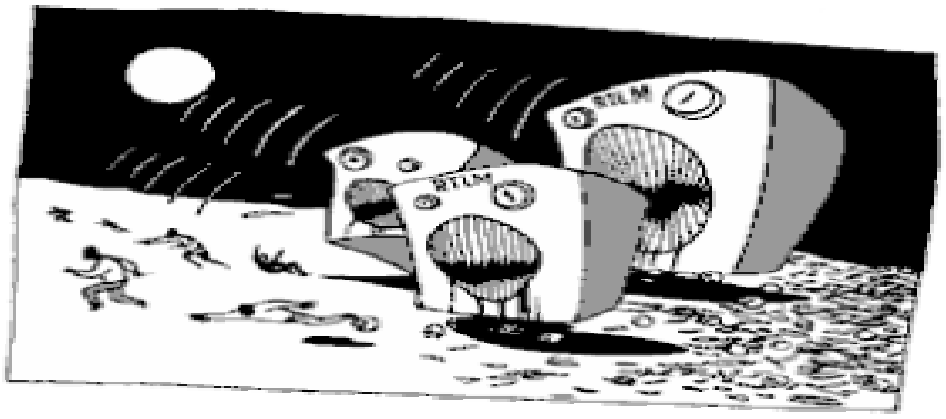

Figure 9. RWANDA POLITICAL CARTOON[130]

The key tool in the genocide was the radio. In 1991, 29 percent of all households had a radio. Prior to and during the genocide, the government distributed free radios to local authorities. Those without radios would listen to broadcast in local bars or the word was passed from neighbor to neighbor. For instance, governmental controlled Radio Rwanda was used mainly be the President and his allies to broadcast false information about the war.[131] With limited radio stations, no television, and government-controlled newspapers, independent verification of events was not possible. The President and his staff controlled the information domain. The RPF also understood the power of the radio and they went on the air soon after the war started. Hutu hard-liners needed a voice. They soon created Radio Television Libre des Mille Collines (RTLM) in April 1993.

---

[130] *Authors Note*: Political Cartoon to support the RTLM. The following summons was transmitted on the RTLM: Everyone who is listening to us rise to the fight for our Rwanda. … Take whatever weapons you have, those who have arrows, take arrows, those who have spears, take spears …We all must fight against Tutsi, we must do away with them, we must destroy them and wipe them off the face of the earth. http://www.yhca.org.md/J9/Rwanda.html

[131] Des Forges, 1999, pp. 68.

RTLM used the airwaves to their fullest extent possible. Not only were instructions on how to conduct acts of genocide, broadcast radio was utilized to recall retired soldiers, summon the personnel needed for special tasks, and offer accounts of the war.[132] Not only were the announcer's voices heard throughout the country, politicians, soldiers, and even clergymen often used radio broadcasts to encourage the killings. The goal of the broadcasts was to highlight the differences in ethnicity of the Hutu and Tutsi tribes. Their messages focused on cruelty, cohesiveness, repression, revolution, and extermination. Furthermore, the radio offered warnings to all. For instance, one address stated, "…those who desert the barriers could expect severe punishments, just as the soldier's who deserted the battlefront."[133] To the international community, the message was clear; these were not acts of genocide, but merely "battles" and "interethnic fighting". Just as organizers used genocide to wage the war, they used the war to disguise the genocide.[134]

IO techniques, including deception and psychological operations were used in Rwanda by the government. Their deception goals were three fold. First, they wanted to mislead foreigners as to the nature of events in order to avoid criticism and perhaps even win support. Next, they wanted to mislead Tutsi to make them easier to kill. Finally, they wanted to engage and manipulate Hutus into participating energetically in the genocidal program.[135] The government accomplished these goals by creating events

[132] Des Forges, 1999, pp. 250.

[133] RTLM, 1994.

[134] Des Forges, 1999, pp. 252

[135] Des Forges, 1999, pp. 252.

to lend credence to propaganda. Also, the idea of "Accusation in a mirror", the idea that one should impute to enemies exactly what one's own faction is planning to do. In other words, the party, which is planning terror, will accuse the enemy of using terror (i.e. psychological operations).[136]

Other methods of IO included the use of public affairs and civilian military operations intended to control the media, foreign aid workers, and UN forces access to information regarding the genocide. For instance, the RPF established close control over foreigners working or traveling in areas under its authority. Information and liaison officers worked hard at shaping the ideas of outsiders while persons employed by foreigners were ordered to report on their activities and conversations. Ordinarily journalists and aid workers were allowed to travel in RPF territory only in the company of officially designated "guides" who sought to ensure that they travel just to approve areas, usually via the main roads. The RPF closed whole regions to UNAMIR and other foreign observers for weeks at a time.[137]

Almost all Information Operations tools were present in Rwanda except for vary technical means such as CNO and EW. This case also serves to remind the planner that IO is more than just technology. Any group or individual regardless of their accessibility to the most current both military and commercial technologies can utilize information operations. Table 10 summarizes IO tools and techniques used in Rwanda. Note the lack of sophisticated

[136] Des Forges, 1999, pp. 66.

[137] FIDH, 1994.

technology based tools, yet the IO campaign was extremely effective and deadly.

IO Method	IO Asset Used	Description/Example
Psychological Warfare	Radio	Two AM radio stations, one FM station based in Kigali
	Television	Only elites had access to limited broadcasts on international concerns
	Newspaper	Demographic majority equals democratic rule thus equals democracy
	Leaflets/ Cartoons	
Propaganda	Radio	Majority rule is democratic rule
	Political Rallies	Incite violence
OPSEC	Physical Theft	Control land development for elites
MILDEC	Confuse foreigners	Limited access to regions during genocide
	Mislead Tutsi civilians	Legitimate government equals legitimate killings
EW	Not present	Not present
IA	Data storage	They kept track of deaths and distributed lists of the names to be killed
Counterdeception	Ruling party agrees to power-	Habyarimana stalls in

	share to please international concerns, however no intention of sharing	**the establishment of a genuine multi-party system with power sharing**
Counterintelligence	**Control on information**	**No more authorizations for travel to adjacent countries, must have permission to change permanent residence**
Physical Destruction	**Sabotage**	**President Habyarimana and the president of Burundi, Cyprien Ntaryamira, are killed their plane is shot down The killings begin**
	Murder	**Killing, and mutilating 10 Belgian soldiers in the UN**
CNO	**Not present**	**Not present**
Civil-Military Affairs	**Control of Foreign Media**	**Via official "guides"**
	Control of Foreign Workers	**Limited area where they could work**
	Control of Foreign Aid agencies	**Limited the area and scope of missions and distribution of critical relief supplies**
	Censorship	**Government controlled media**

Table 10. EXAMPLES OF IO IN RWANDA[138]

[138] Prunier, 1995.

3. Use of Force

The policy makers of the world understood the gravity of the situation almost immediately. Intelligence reports and the media were quick to disseminate the information. However, due to different national interests true action never came. For instance, Belgium was focused on extracting its peacekeepers, the U.S. on avoiding committing resources to crises remote from U.S. concerns, and France wanted to protect its clients and its zone of influence.[139] The UN faired no better. Their goal was simply to broker a cease-fire in the region. Through the UN force, UNAMIR had specific ROE that included direction that they were morally and legally obligated to use all available means to halt ethnically or politically motivated criminal acts, they lacked the troops, training, supplies and experience to truly intervene in the crises.[140] The Rwandan IO plan provided sufficient confusion that nation states and the U.N. were able to avoid responding to the developing crises.

As the carnage continued and a robust response by the U.S. or others was not forthcoming, human rights groups, members of Congress, and others urged the Clinton Administration to counter or "jam" extremist radio broadcasts in Rwanda. These broadcasts spread fear amongst the Rwandan populace, urged participation in the killing, shamed those who sought not to participate, and in many cases, specifically named and provided the whereabouts of those to be killed. As such, the radio broadcasts were essential to the fulfillment of the program of

[139] Des Forges, 1999, pp. 595.

[140] Des Forges, 1999, pp. 596.

extermination. In a memo, Frank Wisner, the number three official at the Pentagon during the crises, acknowledges internal discussions about the feasibility of countering the hate radio were conducted. However, that undertaking the initiative to “jam” the radio would be “ineffective and expensive”; a “wiser” activity would be to assist the “relief effort”.[141]

4. The Genocide Continues

When the genocide occurred, the words Tutsi and Hutu became synonymous with slaughter in the eyes of the international community. For most in the international community outside Africa in 1994, African news is only big news when there are a lot of dead bodies.[142] Other terms such as “tribal war” and “peasant revolt” were used instead of genocide. The United Nations stung by the intervention in Somalia and fearing another ambiguous mission did not take decisive action to intervene.[143] Neither Belgium and France, nor the United States, were serious about intervention because national interests were not at stake. In May 1994, U.N. Secretary-General Boutros-Ghali admitted that the international community had failed the people of Rwanda in not halting the genocide. In 1998, U.S. President Bill Clinton apologized for not having responded to Rwandan cries for help and Secretary-General Kofi Annan also expressed regret. Various other world leaders have acknowledged responsibility for their failure to intervene in the slaughter. The archbishop of Canterbury apologized on behalf of the Anglican Church and the Pope has called

141 Ferroggiaro, 2001.

142 Keane, 1995, pp. 29.

143 Dallaire, 1998, pp. 2.

for clergy who are guilty to have the courage to face the consequences of their crimes.[144]

5. Lessons Learned

Rwanda offers valuable lessons for future conflicts. The use and misuse of information was critical to both sides during the conflict. IO planners must remember that Rwanda teaches that even technologically challenged IO targets can wield enormous amounts of power. Rwanda was not a radical uprising of local farmers and disorganized youths, it was a well planned and executed genocide by those wishing to maintain power. They understood that they lacked the direct military and civil might to control the country, thus they manipulated the population, installing fear and mistrust among them. They utilized the radio, to distribute direction and propaganda, and watched as the genocide unfolded.

Propaganda was again demonstrated to be an extremely dangerous tool when used correctly. For the killers of Rwanda, it was the primary IO tool. Nearly all the tenets of propaganda were used in Rwanda. A lesson for the IO cell is how to recognize and counter propaganda. For effective full dimensional protection, the IO Cell must be aware of the common techniques.

(1) Name Calling: The name-calling technique links a person, or idea, to a negative symbol. The propagandist who uses this technique hopes that the audience will reject the person or the idea on the basis of the negative symbol, instead of looking at the available evidence.

(2) Glittering generalities: "We believe in, fight for, and live by virtue words about which we have deep-set ideas. Such words include civilization, Christianity, good, proper, right, democracy,

[144] Des Flores, 1999, pp. 254.

patriotism, motherhood, fatherhood, science, medicine, health, and love.

(3) Euphemism: When propagandists use glittering generalities and name-calling symbols, they are attempting to arouse their audience with vivid, emotionally suggestive words. In certain situations, however, the propagandist attempts to pacify the audience in order to make an unpleasant reality more palatable. This is accomplished by using words that are bland and euphemistic.

(4) Transfer: Is a device by which the propagandist carries over the authority, sanction, and prestige of something we respect and revere to something he would have us accept. For example, most of us respect and revere our church and our nation. If the propagandist succeeds in getting church or nation to approve a campaign in behalf of some program, he thereby transfers its authority, sanction, and prestige to that program. Thus, we may accept something, which otherwise we might reject.

(5) Bandwagon: He appeals to the desire, common to most of us, to follow the crowd. Because he wants us to follow the crowd in masses, he directs his appeal to groups held together already by common ties, ties of nationality, religion, race, sex, vocation.

(6) Fear: When a propagandist warns members of her audience that disaster will result if they do not follow a particular course of action, she is using the fear appeal. By playing on the audience's deep-seated fears, practitioners of this technique hope to redirect attention away from the merits of a particular proposal and toward steps that can be taken to reduce the fear.[145]

The second lesson learned that Rwanda offers is an insight into civil-military and public affairs operations. Rwanda military and civilian officials controlled the information that would flow between the entities of the media, relief workers, and diplomats. Furthermore, they

[145] LSU, 2003.

were very careful to create what was shown and the information that was leaked to any one element. For instance, it became clear that blanket genocide would eventually be resisted and they took active steps to cover these actions. Thus the Rwandan government instituted a process of selected killings or “pacification” killings. The pacification killings were an attempt to target selected groups or individuals. Their attempt to shift the target was also used as an example to show that they were stopping the genocide. However, this was just another deception operation. Authorities drove through Butare town and its environs beginning on April 23, making announcements over a sound system or through a hand-held megaphone. One announcement said, “signs of the killing must be hidden from journalists flying over in helicopters and from surveillance satellites passing overhead”. [146] The IO Cell must be alert to shifts in process or plans within an AOR. These shifts can drastically change the nature of the IO plan or the target audience.

The final lesson learned in Rwanda related to IO involves the message itself. MPAT planners must understand what are the critical information messages of the adversary and what the opponent’s objectives. For example, the goal of the main message in Rwanda was to split the society on racial ideologies. Early in the campaign, the propagandists relied heavily on the idea that the Hutu and Tutsi where radically different. Next, the message relayed informed the population that they must exterminate Tutsi killers before they kill Hutus. Finally, the propagandists stressed that Tutsi were foreign to the area and had stolen Rwanda from

[146] FIDH, 1995.

its rightful inhabitants.[147] When IO operators receive intelligence reports regarding opposition messages within the AOR, they must examine them for the following ideas or themes:

(1) Unity: The state or quality of being in accord or harmony. The idea of a homogenous culture. For instance in Rwanda, propaganda included, “A cockroach cannot give birth to a butterfly.”

(2) Infiltration: To penetrate with hostile intent. For example, in Rwanda “It is because of this Tutsi infiltration into society that the country has no more secrets and they have been able to invade it with no trouble at all.”

(3) Restoring Old Regimes: A form of government, normally fascist. In defining the “enemy,” the military high command focused on those Tutsi “who refused to accept the revolution and wanted to re conquer power by any means.”

(4) Genocide: The systematic and planned extermination of an entire national, racial, political, or ethnic group. They insisted that not just the freedom and prosperity of Hutu were at risk but their very lives. They warned that the Tutsi minority could not hope to reestablish their control over the majority without killing large numbers of Hutu

(5) Innocent Victim: One who is harmed by or made to suffer from an act, circumstance, agency, or condition: victims of war. Underlying much of this propaganda is the image of the Hutu as the innocent victim—victim of the original aggression by Tutsi conquerors some centuries ago, of the “infiltration” of the state and society, and of the 1990 invasion.

(6) They Cause Their Own Misfortune: Ill luck. According to the propagandists, the suffering of the Hutu was real and grievous, but the misery of the Tutsi was a sham or, if real, had been their own fault.

[147] Des Flores, 1999, pp.465.

Most information messages will fall into one or more of these categories with regards to psychological control of the population. When IO warriors review the such propaganda, they must insure that IO plans should be devised that counter these elements of propaganda.

C. SUMMARY

Rwanda from an information operations perspective is a valuable case for future IO operators to examine and understand. The case itself offers valuable insight into the dangerous of information operations when backed by government policies, process, money, and technology.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CASE STUDY INTERACTION WITH IO ANNEX

A. INTRODUCTION

This chapter serves to illustrate the potential utility of the proposed IO Annex information by examining the war in Rwanda. By using the IO Annex, it is possible to flush out IO themes, potential targets, and courses of actions (both friendly and enemy) that may be useful to IO planners. The IO elements described in the case study offer evidence that the IO Annex is an effective framework for multi-national counter operations in the future.

B. EARLY WARNING

If international organizations are to be involved in crises situations, they will have to overhaul their intelligence capabilities.[148] Information Operations (IO) and its interactions with Information Support and Management allow for increased situational awareness. The IO actions prevalent in Rwanda fall nicely into the MPAT definition. For instance, MPAT focuses on IO that influences decision making processes of political, military, and social entities while protecting one's own. In Rwanda, Hutu extremists lacked the ability to control the division of their country, thus they sought to control the message with-in their country. Not only was the message well controlled, it was propagated through simple means and constantly re-enforced throughout the genocide. An examination of the Hutus' actions from an IO perspective would have made it more difficult for the genocide to be disguised as civil strife.

[148] Feil, 1998, pp. 27.

For the IO Annex to be effective in identifying the overall themes of the genocide, planners would have had to rely on Intelligence Support. The thoroughness of the intelligence, evaluation, and identification would have determined how rapidly appropriate response planning could have been prepared. There was no lack of intelligence reports both open and closed sources regarding the situation in Rwanda. As much as the Hutu extremists attempted to control the flow of information out of the country, they ultimately failed because the world has almost instant connectivity to events due to the media and the Internet.

For successful utilization of the Annex, planners must rely on early warning of potential disaster. Early warning is the collection, analysis and communication of the relevant evidence and conclusions to policy-makers to enable them to make strategic choices. Unlike traditional intelligence, which also collects and analyzes information and communicates the results, the object of early warning is not primarily security for one's self or one's country, but the security of another; in early warning, the security is not self-directed. The other party or parties are not presumed to be adversaries, as is the case with intelligence analysis.[149] The IO Annex identifies that intelligence support will drive the Information Operations and that early warning is a primary consideration. This IS will help define campaign objectives for IO attacks and counter operations.

C. POTENTIAL TARGETS

IO targets for the MPAT fall into three distinct categories. First the Leadership target including civilian, social, military, and cultural targets. Second, military infrastructure targets include communications, intelligence, logistics, operations, and weapons systems. And finally, the civil infrastructure targets include telecommunications, transportation, energy, economic, and manufacturing. The IO ANNEX identifies the latter as the most likely and most critical targets that an opponent may target during MOOTW offensive information operations. For instance, in Rwanda, the lack of significant military and civilian infrastructure drove the leaders of the genocide to target the first the leadership of the opposition and eventually the entire civilian population of the opposition. They returned to only targeted killings that would have the most influential effects on the population. Using the IO Annex, planners would have identified and countered the targets enabling the Rwandan operations.

The IO Annex identifies targets in offensive IO in three distinct categories: the global information infrastructure (GII), national information infrastructure (NII), and the defense information structure (DII). Each of these categories identified by the IO Annex describe one or more of the entities targeted during the genocide. For planners and operators, counter action against all three could have been accomplished if the IO SOP was utilized. For instance, threats to any force intervening in Rwanda in 1994 could have been expected from both belligerents and armed civilians, lightly armed militia, combat forces of

the RPF, and political parties.[150] Each of these groups has been identified in the IO Annex as potential targets of MPAT IO. Each group or entity make-up or influence the GII, NII, and/or the DII.

D. COURSES OF ACTION

The rapid introduction of force in Rwanda presupposes some definable end to be achieved and the will to achieve that end in a reasonable amount of time.[151] A critical consideration in any IO campaign are the limitation of time, space, and force. For the Annex to be effective in cases, such as Rwanda, a clear understanding of these elements is crucial. For example, each potential course of action, either friendly or enemy, can easily be deduced using the IO Annex task selection matrix included in the SOP. The cell can quickly identify large strategic operations. Based on time restraints during operations, the ability of the planner to drill down to more and more specific IO options are also easily accomplished.

Currently, the UN lacks the capability to respond rapidly in concrete ways to deteriorating situations around the world.[152] The IO Annex is built upon the idea of the rapid activation of a CCTF Headquarters at the request of a host nation. It is not a stretch to assume that the entire SOP including the IO portion is useful to other organizations such as the United Nations or Organization of African States if the supporting infrastructure is put into place or the operation is supported by U.S. led coalition.

---

[150] Feil, 1998, pp. 7.

[151] Feil, 1998, pp. 11.

[152] Feil, 1998, pp. 12.

Clearly any action by the CCTF in Rwanda would fall distinctly into the uncertain environment of MOOTW. MOOTW in the uncertain environment is one in which the control, intent, and capability of host nation and hostile forces are unknown or uncertain. The type of IO required may also be uncertain. However, to counter IO actions in Rwanda, the IO Annex specifies that social interaction challenges will focus on civil-military operations or planned activities in support of military operations that enhance the relationship between the military forces and civilian authorities and population and which promote the development of favorable emotions, attitudes, or behavior in neutral, friendly, or hostile groups. IO actions would have focused on the social interactions of the CCTF IO Cell and civil-military relations with-in the Rwandan AOR. The IO Annex identifies this as a potential challenges during operations and if IO planners understand this, then their ability to foresee such limitations would have been greatly enhanced.

E. DECONFLICTION OF IO

Public affairs (PA) are public information, command information, and community relations' activities directed toward both the external and internal publics. The evidence supports the claim that Public Affairs actions with-in Rwanda during the genocide would have been crucial to the IO actions against any group or individual because the control of information throughout Rwanda was the key to successful actions of the Hutu leadership. For example, the pro-Hayabarimana publication *La Medaille Nyiramacibiri* discounted reports that Hutu officials had been responsible for killing Tutsi and offered instead to give readers lists of the Hut killed by Tutsi so, "then you will know who are

the real criminals."[153] These types of actions are a combination of public affairs, psychological operations and military deception. The IO warrior must be aware that the combination of IO actions can be prevalent in numerous forms and may not distinctly fall into one category or another. This complicates IO actions because one's action against psychological operations may counter one's actions against public affair operations. The deconfliction issue is crucial to successful operations. The IO Annex provides an IO cell structure that provides a format for deconfliction of IO actions in the AOR.

F. POSSIBLE IO AGAINST THE GENOCIDE

Introducing force into Rwanda would have had to revolve around the nature and structure of multinational nature of peacekeeping or peace enforcement missions. A robust communications capabilities, civil-military operations personnel, psychological operations staff, interpreters, and intelligence analysis cells would have been vital to the success of such a complex operation.[154] To support such actions the IO Annex identifies the above cells as critical to mission accomplishment and provides a process for planning actions to counter the Hutu's IO.

Using the IO Annex Task selection tool it is clear , which IO actions would have had an effect on the genocide in Rwanda and which actions would have been useless. First, any CNO actions would have failed because Rwanda itself offers no viable targets. In 1994, the country had limited computers and no Internet connections available. However, technical means such as EW would have been vary effective

[153] Des Forges, 1999.

[154] Feil, 1998, pp. 19.

in jamming air waves especially those used for radio propaganda. Second, psychological operations directed against both parties would have been effective to counter propaganda because the entire genocide revolved around influence operations. Third, reconnaissance and surveillance capabilities would be essential for forces engaged in mobile operations as well as for the security of the force.[155]

G. SUMMARY

The need for a response mechanism of other humanitarian catastrophes now and into the future will continue to drive the evolution of the IO Annex. Rwanda and the IO conducted prior to and during the genocide only serve to remind us that IO can and will continue to be a deadly and effective tool in future military operations. The overall strategy that would have been useful against the genocide in Rwanda would provide direction about: 1) the message to be passed, 2) the intended audience(s), 3) the unintended audience(s), 4) how to pass the message, and 5) how to reduce the effectiveness of the opponents information operations.[156]

More than 2,300 years ago, the ancient Chinese strategist Sun Tzu appreciated values, interests, and the rational comparison of power. Before launching a military campaign, he said that the temple council should compare unity on the home front and the morale of the army with that of the enemy. He was also convinced that careful planning based on information would contribute to speedy victory.157 The IO Annex could have provided the framework

[155] Feil, 1998, pp. 20.

[156] Morthland, 2002.

[157] Tzu, 1971. pp. 39-40.

for such planning in Rwanda and does offers such a framework for future operations.

VI. PROPOSED IO MPAT SOP ANNEX SUMMARY

A. INTRODUCTION

The need for MPAT SOP IO Annex grew out of the evolution of information warfare and the increased requirement for coalition operations. It was created via inputs from senior officers of 150 nations during semi-annual MPAT conferences. Each officer had varying levels of experience both in military operations and information operations. Some had never heard of IO, others were very well versed. However, all had years of experience in military strategic planning and implementation of a variety of operations. Two goals where set for the creation and implementation of the Annex. First, MPAT planners wanted to create a usable Annex to support rapid IO planning mainly during Crises Action Planning (CAP) that included a streamlined and user-friendly IO task selection tool to help plan IO COA's. Second, they wanted to create a document that would help commanders and operators understand the unique aspects of MNF IO to include the identification possible limitations and challenges when operating in the MNF environment.

B. THEORY

The IO Annex revolves around the idea presented in Chapters I through IV and is based largely on Waltz's work.[158] This thesis served as an exploratory tool to create the Annex. As mentioned earlier in Chapter I, information operations extend beyond the information realm; IO also deals with the physical, information infrastructure, and perceptual realms. The interactions of the three real

[158] Waltz, 1998, pp. 117.

dealing with information content and process form the basic functional model of warfare.[159] The physical realms are the physical items that may be attack as a means to influence information. The information infrastructure realm deals with the information content or process that may be attacked electronically to directly influence the information process or content without physical impact on the target. The perceptual realms are attacks that may be directly targeted on the human mind through electronic, printed, or oral transmission paths.

The three realms, as described by Waltz, support the first goal of the MPAT because they offer the framework required to tailor the MNF IO Annex. The first goal was to support Crises Action Planning. The IO Annex has accomplished this goal by creating:

(1) A straightforward user-friendly design Annex.

(2) IO definitions suitable for MNF operations.

(3) Simple IO Cell design including numerous non-IO members involved in IO planning (such Intel, PAO, and Legal).

(4) Supplemented Host Nation IO planning and strategic guidance.

(5) Including all IO definitions and elements.

(6) Including IO Cell structure and responsibilities

(7) Including Risk/Benefit/Cost calculations matrixes.

(8) Including additional planning guidance, limitation and challenges of IO.

The second goal was to create a document that would help commanders and operators understand the unique aspects

[159] Waltz, 1998, pp. 27.

of MNF IO and create a user-friendly IO task selection tool to help plan IO COA's. This goal was accomplished by including in the IO Annex the following:

(1) Input into overall MNF COA development.

(2) Calculations of the probabilities associated with COA and ECOA.

(3) Additional guidance for COA development.

(4) Additional information on possible IO actions, limitations and challenges of each COA or ECOA.

(5) Questions to aid commanders in the decision cycle.

(6) A mechanism to assist operators and planners cover all the unique aspects of IO in one documents.

(7) Non-trained IO planners and operators the ability to understand the basics of IO.

(8) Limitations and challenges for IO selection.

C. PROPOSED SOP IO ANNEX

The proposed SOP utilizes the created MPAT generated IO definition presented in chapter I. "IO are actions taken to effect information, information systems, and influence decision making processes of political, military, and social entities while protecting one's own. IO spans the entire spectrum from peace, to crisis, to conflict, to restoration". The definition highlights the idea that offensive and defensive IO goes beyond technology and focuses of political, military, and social entities of the decision cycle. These entities and actions against them are driven by unity of purpose, effort, and interoperability.

1. Purpose

The purpose of the annex is to provide a description of the CCTF Information Operations Working Group (IOWG),

its responsibilities, and procedures for conducting successful IO. The annex specifies methods for the establishment an IOWG. All efforts executed by the Coalition/Combined Task Force (CCTF) IOWG must be coordinated within the CCTF and with the Supported Strategic Commander's overarching IO policies and guidance. The CCTF IOWG is organized to ensure that a broad range of IO actions and activities are integrated into the CCTF planning process, coordinated with ongoing or planned operations, and contribute to the CCTF's intent and desired end states.

2. Responsibilities

The CCTF C3 is the principle staff element responsible for embedding IO into the Coalition/Combined Planning Group (CPG) process and ensuring that IO is properly integrated and coordinated throughout all operational phases. The CCTF IOWG is composed of select representatives from the staff and from supporting agencies/organizations and is responsible to the CCTF C3 for planning, integration, coordination, monitoring, and assessment of the Information Environment (IE) within the AO. Coordination of operational and strategic IO objectives with the Supported Strategic Commander's IOWG is essential. The CCTF C3 must integrate IO target concerns and target nominations into the planning and execution cycle of the targeting process. Other responsibilities and duties of the IOWG include:

(1) Incorporate Lead Nation's National Command Authorities guidance and the Multinational Force Strategy for the MNF partners into IO objectives in support of strategic goals.

(2) Coordinate with the media and public relations office for the Lead Nation National Command

Authorities and the Supported Strategic Commander (for example CCTF Public Affairs Office).

(3) Coordinate IO related guidance for:
   a. Physical Destruction
   b. Electronic Warfare (EW)
   c. Computer Network Operations (CNO): for example Computer Network Attack (CNA), Computer
   d. Network Defense (CND), and Cyber Warfare
   e. Psychological Operations (PSYOPS)
   f. Operations Security (OPSEC) and Military Deception (MILDEC)
   g. Public Affairs (PA)
   h. Other capabilities and functions.

(4) Coordinates with all staff elements to shape the impact of CCTF actions on the adversary's perception and ability to operate.

(5) Draw upon the capabilities of other coalition military organizations, government, and non-government agencies as necessary to obtain information for planning and operational considerations.

(6) Provide a representative to the C5 Future Plans and FOPS to advise on the development of IO related guidance for the CCTF.

3. Process

Employment of IO begins with articulating and understanding the CCTF's mission, concept of operations, objectives, and intent. The same fundamentals of campaign planning apply to the IO portion of the plan. Specifically, the working group will provide detailed concepts of IO operations for supporting CCTF objectives. The operational level links the tactical employment of IO to strategic objectives. Furthermore, the IOWG will coordinate, integrate, analyze, and develop the IO plan. The IOWG will coordinate and integrate the CCTF IO Campaign Plan into the CCTF OPORD or Campaign Plan. Additionally,

the IOWG will conduct extensive mission analysis of IO operations within the spectrum of MOOTW and SSC. The IOWG will also develop IO objectives based on guidance from the CCTF. Finally, the IO Cell will review and determine the targets, areas of influence, or audiences that are to be the focus of IO actions.

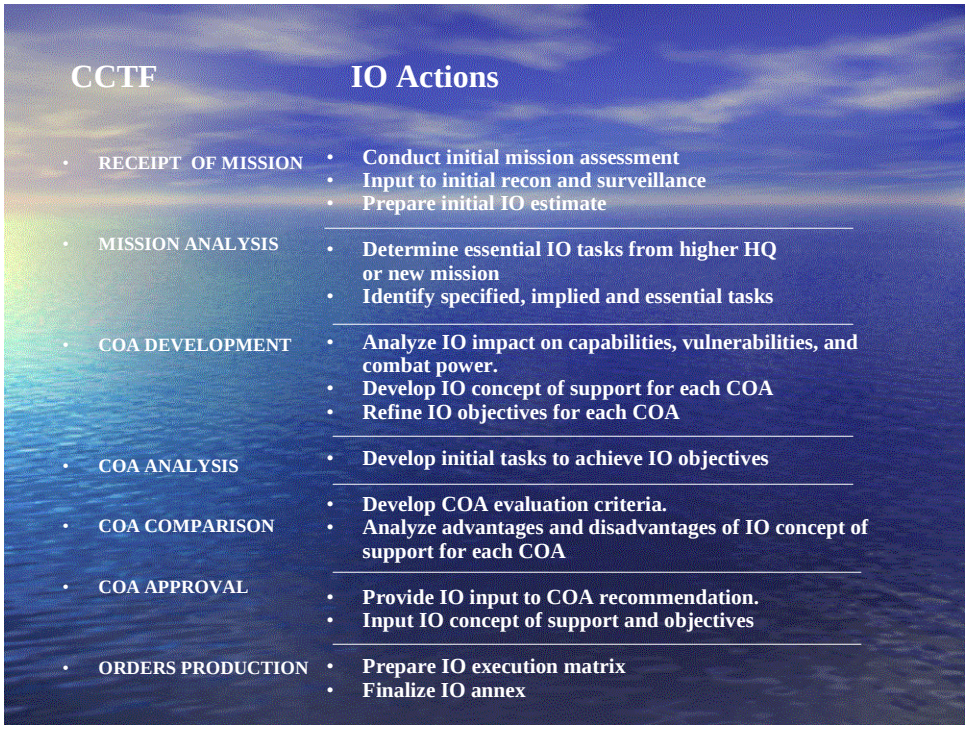

Figure 10. CCTF IO ACTIONS

4. CCTFG IOWG Procedures

The Annex directs the development of IO operations and the associated delivery methods needed to achieve defined objectives against specified targets IO in the CCTF can be accomplished by Influence and/or Electronic approaches. For offensive IO and precision engagement, the CCTF IOWG requires intelligence to support planning and control of operations for offensive IO to include efforts to shape and influence perceptions, computer network attack or other courses of action taken against adversaries. The CCTF IOWG

must define campaign objectives for IO attacks, and monitor, coordinate, and integrate component activities to identify targets and target access, assess the target's vulnerabilities, select the optimum IO attack and provide Measures of Effectiveness (MOE) and Battle Damage Assessment (BDA). For defensive IO and full dimensional protection, the CCTF IOWG needs to know adversary IO attack capabilities (if any) to facilitate defensive and information assurance programs. It is imperative that the CCTF IOWG submits intelligence requirements as early as possible after CCTF establishment. The following procedures are incorporated and should be utilized by the MNF:

(1) SITUATION

a. Enemy. Identify enemy IO C2 nodes and the vulnerability of those nodes

i. Terrain. List terrain aspect as affecting each of the IO elements.

ii. Weather. List weather aspects as affecting each of the IO elements.

iii. Enemy IO capabilities

iv. Identify enemy IO elements.

v. Identify enemy C2 vulnerabilities.

vi. Identify enemy capabilities to degrade friendly C2.

vii. Identify the enemy situation, force disposition, intelligence elements, and possible actions.

viii. Identify specific information that bears directly on the planned IO.

b. Friendly. Identify IO elements and their vulnerability to enemy actions.

i. Identify IO capabilities to degrade enemy C2.

ii. Identify IO assets needed to attack enemy targets.

iii. Identify the friendly forces that will directly affect information superiority.

iv. Identify the critical limitations of planned IO.

c. Attachments and detachments.
    i. List IO assets that are attached or detached.
    ii. List IO resources available from higher headquarters.

(2) MISSION: State the mission of IO in support of the CCTF.

(3) EXECUTION
a. Scheme of support.
    i. Describe the IO concept of support, IO objective, and tasks to the IO elements. Complex IO concept of support may require a schematic to show IO objectives and IO task relationships.
    ii. Include a discussion of the overall IO concept of support, with the specific details in either subparagraphs or appendixes.
b. Execution Matrix. Refer to execution matrix to clarify the timing relationship among various IO tasks. This annex should contain the information to synchronize timing relationship of each of the elements IO and the related IO activities of PA and CA.
c. Operations Security (OPSEC). State how the OPSEC objectives and OPSEC tasks will deny the enemy information based on the approved COA. Emphasis is on denying the enemy accesses to his own or foreign intelligence elements. Identify target sets and desired effect, by priority, for OPSEC. Synchronize this element with the other IO elements.
d. Psychological Operations (PSYOP). State how the PSYOP objectives and PSYOP tasks will degrade, disrupt deny, or influence the enemy based on the approved COA. Identify the audiences, and desired effect, by priority, for PSYOP. Synchronize this element with the other IO elements.
e. Military deception (MILDEC). State how the military deception objectives and military deception tasks will deceive, and influence the enemy based on the approved COA. Synchronize this element with the other IO elements.
f. Electronic Warfare (EW). State how the EW objectives and EW tasks will degrade, disrupt,

deny, and deceive the enemy based on the approved COA. State the defensive and offensive EW measures. Identify target sets and effect, by priority, for EW operations. Synchronize this element with the other IO elements.

g. Information Assurance (IA). State how the IA objectives and IA tasks will deny the enemy access to our C4 based on the approved COA. Identify the information and INFOSYS for protection. Synchronize this element with the other IO elements.

h. Counterdeception. State how the counterdeception objectives and counterdeception tasks will disrupt, deny and exploit the enemy based on the approved COA. Identify the units for protection. Synchronize this element with the other IO elements. Refer to Annex B, Intelligence, for detailed counterdeception information.

i. Counterintelligence. State how the counterintelligence objectives and counterintelligence tasks will degrade, disrupt, deny and exploit the enemy based on the approved COA. Identify the units for protection. Synchronize this element with the other IO elements. Refer to Annex B, Intelligence, for detailed counterintelligence information.

j. Counter propaganda. State how the counter propaganda objectives and counter propaganda tasks will degrade, disrupt, deny and exploit the enemy based on the approved COA. Identify the units for protection. Synchronize this element with the other IO elements.

k. Physical destruction. State how the physical destruction objectives and physical destruction tasks will destroy, degrade, disrupt, and deny the enemy based on the approved COA. Identify target sets and effect, by priority, for destruction. Synchronize this element with the other IO elements.

l. Computer network attack (CNO). State how the CNO objectives and CNO tasks will destroy, degrade, disrupt, and deny the enemy based on the approved COA. Identify target sets and effect, by priority, for attack. Synchronize this element with the other IO elements.

m. Physical Security. State how the physical security objectives and physical security tasks

will deny the enemy based on the approved COA. Synchronize this element with the other IO elements.

n. Special Information Operations. SIO may be classified. Access is restricted to strict need to know. Synchronize this element with the other IO elements.
o. Civil Affairs (CA). CA is a related activity to IO. State the IO objectives for CA.
p. Public Affairs (PA). PA is a related activity to IO. State the IO objectives for PA.

5. Additional Considerations

Conducting Combined/Coalition Information Operations can present classification challenges that must be addressed during combined planning. Use of the Coalition Coordination Center (CCC) can greatly assist in this process. The specific manning requirements and number of augmenters to the CCTF IOWG should be tailored to meet mission requirements identified in Crisis Action Planning. Upon standing up the CCTF, identify early on communications connectivity requirements for support to the CCTF IOWG. It is imperative that IO initiatives are coordinated and approved as early as possible when the CCTF is activated. Various IO products, such as CNA and PSYOPS, require approval at the Lead Nation, supporting nations and/or at strategic levels.

D. INTERPRETATION OF PROCEDURES

The simple straightforward approach to IO presented above focuses on technology, procedures, and policy. In order to be successful, all three of these elements must in balance within the CCTF. As important as hardware may be, innovative doctrine, tactics, training, and organizations must be developed and refined in a process of transforming military operations for the information age.[160] Not all

[160] Gompert, Kugler, & Libicki, 1999, pp. 3.

problems that will be faced by the MNF will find solutions in technology. Furthermore, the level of technology may not be the most important factor.[161] Procedures and policies may also be the limiting factor when dealing with IO. For instance, each the host nation is limited by bandwidth internal to the CCTF, a technological fix may not be possible. Planners must turn to policy and procedures to find work-around to the problem.

E. SUMMARY

New technology alone does not revolutionize warfare. Rather, technology's impact on systems evolution, operational tactics, and organizational structure is its true advantage.[162] This fuels necessary and complementary changes in doctrine and organizational structure. It may be a simple as limiting the amount of data passed on the lines, limiting users to specific times, or outsourcing intelligence requirements.

[161] White, 1996, pp. 54.

[162] Krepinevich, 1995, pp. 163-64.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

A. INTRODUCTION

This thesis explained the rational associated with the creation of a useable MNF MPAT IO Annex for use during MOOTW and SCC. In order to be more useful in the future, a summary of findings, the limitations of this study is, and a section dedicated to follow-on research is included to stimulate continued research and discussion in support of mutli-national IO.

B. SUMMARY OF FINDINGS

The findings of the research indicate four main points. First, IO in the MNF relies heavily on U.S. centric approach to operations. This is due to the large doctrinal and technology gaps between member nations. Second, most foreign members of the MPAT see IO as a technological weapon and if they do not possess the technology they believe they cannot participate in operations. Third, IO must have the ability to utilize the physical destruction of the target to accomplish operational goals. Physical destruction can remain in the traditional war fighter realm; however IO operators must understand that it is a viable option or hindrance. Finally, the concepts of precision engagement and full dimensional protection apply to IO.

C. PREDICTIONS

For future operations in the MPAT or any MNF environment, IO will continue to evolve as a distinct and separate form of warfare. First, IO will become a larger and more integrated part of MNF operations. Second, more MNF member nations will turn to the unique elements of IO

to meet operational objective. Third, MNF members will attempt to close the U.S. lead associated with technologies dealing with information operations. Finally, CNO will play and ever increasing role and may eventually dominates IO actions as the use of technology in member nations increase.

D. VALIDATION/LIMITATIONS OF STUDY

The actual use of the IO Annex has never been proven in real world or exercise operations. However, the U.S. Pacific Command has adopted portions of the IO Annex created during MPAT conferences. Many of the military and IO principles, challenges, and limitations have been proven over time. Furthermore, the case study does offer a validation of the procedures presented. The goal was to advance the study Information Operations and provide the bases for a document that could be used during multinational operations. The key principles of precision engagement and dimension defense are not new, however there are almost no studies regarding these principles with the application of IO. If a solid baseline for the IO Annex of the MPAT SOP was created during the study, the author has succeeded.

E. PROPOSED FOLLOW-ON RESEARCH

To improve upon this work, future reviews and research is required in several different areas. First, continues review of the SOP by MPAT members during scheduled conferences is required. The IO Annex included in this research is not static. The entire field of IO and its relation to operations is an evolving field of study. The annex created should serve as a starting point for future reviews and operations; it is not intended to be a dynamic fixture for IO planners and operators.

Second, lesson lessons learned from actual operations and follow-on conferences should be incorporated into future reviews and new editions of the IO Annex. Only useful inputs from actual real world operations will serve to further the usefulness of the IO Annex.

Finally, an in-depth study on the technical limitations of MPAT member nations is required to further the creation of the annex. Additional studies in the technical limitations offers planners the ability to focus on what technological are available for operations in the MPAT organization and may avoid delays in assembly effective coalition IO teams when required.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: INTRODUCTION/SUMMARY

The below included appendices were created via the inputs of numerous officers from a host of Asian-Pacific countries led by the U.S. Pacific Command's MPAT organization. Annex D is the accumulation of MPAT inputs from 2003-2004. The author, to further the operational readiness and completeness of the SOP, created the additional annexes.

Annex D

INFORMATION OPERATIONS

Chapter C-3 OPERATIONS

A. Purpose

1. Information Operations (IO) are actions taken to affect friendly, neutral and adversary / threat information and information systems while protecting one's own information and information systems. IO spans the entire spectrum from peace, to crisis, to conflict, to restoration and may be offensive and/or defensive in nature.

   a. Offensive Information Operations are acts conducted to meet strategic, operational, or tactical objectives. The operations may be performed covertly, without notice to the target, or they may be intrusive, disruptive, and even destructive. The effects on information may bring physical results that are lethal to humans.
   b. Defensive Information Operations are those actions that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

2. Information Operations are comprised of Core Capabilities and enabled by Supporting and Related Capabilities.

   c. **IO Core Capabilities**: Electronic Warfare (EW), Computer Network Operations (CNO), Operations Security (OPSEC), Military Deception (MILDEC), and Psychological Operations (PSYOPS).
   d. **IO Supporting Capabilities**: Information Assurance (IA), Physical Security, Counterintelligence (CI) and Physical Attack and/or Destruction.
   e. **Related Capabilities**: Public Affairs (PA) and Civil-Military Operations (CMO).

3. This annex provides a description of Coalition/Combined Task Force (CTF) Information Operations, the Information Operations Cell (IO Cell), Information Operations Working Group (IOWG), their responsibilities, and IO planning process. CTF IO Cell and Working Group efforts must be coordinated within the CTF and with the Supported Strategic Commander's overarching IO policies and guidance.

4. The CTF IO Cell and IOWG are organized to ensure that a broad range of IO actions and activities are integrated into the CTF planning process, coordinated with ongoing or planned operations, and contributing to the CCTF's intent and end states.

B. Organization

1. **CTF Operations (C3).** The CTF C3 is the principle staff element responsible for embedding IO into the Coalition/Combined Planning Group (CPG) process and ensuring that IO is properly integrated and coordinated throughout all operational phases.

2. **CTF Information Operations Cell (IO Cell).** The CTF Commander or C3 will establish an IO Cell. The IO Cell is comprised of a core group of planners from within the headquarters staff and resides within the C3. The IO Cell is the focal point for IO planning to include coordination, integration and de-confliction. The IO Cell must be represented in the CTF IOWG (if established), COPS, FOPS and C5 Plans. Early and continuous exchange of information and close coordination of planning activities between the IO Cell, IOWG, COPS, FOPS, and C5 Plans is essential to successful integration of IO planning process.

3. **CTF Information Operations Working Group (IOWG).** The CTF Commander or C3 may establish a CTF IOWG. The IOWG is comprised of members from the IO Cell and select representatives from the staff and supporting agencies/organizations. The IOWG is responsible for supporting IO Cell planning, integration, coordination, monitoring, and assessment of the Information Environment (IE) within the AO.

Coordination of operational and strategic IO objectives with the Supported Strategic Commander's IOWG is essential.

a. Integrate IO target concerns and target nominations into the planning and execution cycle of the targeting process.
b. Incorporate Lead Nation's National Command Authorities guidance and the Multinational Force Strategy for the MNF partners into IO objectives in support of strategic goals.
c. Coordinate with the media and public relations office for the Lead Nation National Command Authorities and the Supported Strategic Commander (for example CCTF Public Affairs Office).
d. Coordinate IO related guidance for:

   i. Physical Destruction
   ii. Electronic Warfare (EW)
   iii. Computer Network Operations (CNO): for example Computer Network Attack (CNA), Computer
   iv. Network Defense (CND), and Cyber Warfare
   v. Psychological Operations (PSYOPS)
   vi. Operations Security (OPSEC) and Military Deception (MILDEC)
   vii. Public Affairs (PA)
   viii. Other capabilities and functions.

e. Coordinates with all staff elements to shape the impact of CCTF actions on the adversary's perception and ability to operate.
f. Draws upon the capabilities of other coalition military organizations, government, and non-government agencies as necessary to obtain information for planning and operational considerations.
   ? g. Provide a representative to the C5 Future Plans and FOPS to advise on the development of IO related guidance for the CCTF.

C. Process. Information Operations impacts all aspects of CTF Operations and must be coordinated and integrated into the CTF OPORD or Campaign plan. Employment of IO begins with mission analysis: articulating and understanding the CTF's mission, concept of operations, objectives, and intent. A well-developed and synchronized IO plan will result in a detailed concept of IO to support strategic, operational and tactical objectives. Specifically, the operational IO process will:

1. Result in extensive mission analysis of IO within the spectrum of MOOTW and SSC.

2. Develop and/or integrate objectives based on guidance from the following sources:

   a. UN Mandate or other Strategic Guidance
   b. Lead Nation
   c. Supported Strategic Commander
   d. CTF strategy
   e. Commanders Intent
   f. Other sources as directed

3. Review and refine the objectives, areas of influence, or audiences that are the focus of IO actions. Examples include:

   a. Leadership
      (1) Civilian
      (2) Social
      (3) Military
      (4) Cultural

   b. General Populous
      (1) International
      (2) Regional
      (3) Local

c. Military Infrastructure
   (1) Communications
   (2) Intelligence
   (3) Logistics
   (4) Operations
   (5) Weapons systems

d. Civil Infrastructure
   (1) Telecommunications
   (2) Transportation
   (3) Energy
   (4) Economic
   (5) Manufacturing

4. Once IO objectives are identified and prioritized, an IO objective folder will be prepared and methods of delivery will be determined.
   a. Define the environment.
      i. Enemy. Identify enemy IO C2 nodes and the vulnerability of those nodes.
      ii. Terrain. List terrain aspect as affecting each of the IO elements.
      iii. Weather. List weather aspects as affecting each of the IO elements.
   b. Enemy IO capabilities
      i. Identify enemy IO elements.
      ii. Identify enemy C2 vulnerabilities.
      iii. Identify enemy capabilities to degrade friendly C2.
      iv. Identify the enemy situation, force disposition, intelligence elements, and possible actions.
      v. Identify specific information that bears directly on the planned IO.
   c. Friendly. Identify IO elements and their vulnerability to enemy actions.
      i. Identify IO capabilities to degrade enemy C2.
      ii. Identify IO assets needed to attack enemy targets.
      iii. Identify the friendly forces that will directly affect information superiority.
      iv. Identify the critical limitations of planned IO.
   d. Attachments and detachments.
      i. List IO assets that are attached or detached.
      ii. List IO resources available from higher headquarters.
   e. Execution:
      i. Describe the IO concept of support, IO objective, and tasks to the IO elements. Complex IO concept of support may require a schematic to show IO objectives and IO task relationships.
      ii. Include a discussion of the overall IO concept of support, with the specific details in either subparagraphs or appendixes.
      iii. Refer to execution matrix to clarify the timing relationship among various IO tasks. This annex should contain the information to synchronize timing relationship of each of the elements IO and the related IO activities of PA and CA.
   f. Guidance for:
      i. Operations Security (OPSEC). State how the OPSEC objectives and OPSEC tasks will deny the enemy information based on the approved COA. Emphasis is on denying the enemy accesses to his own or foreign intelligence elements. Identify target sets and desired effect, by priority, for OPSEC. Synchronize this element with the other IO elements.
      ii. Psychological Operations (PSYOP). State how the PSYOP objectives and PSYOP tasks will degrade, disrupt deny, or influence the enemy based on the approved COA. Identify the audiences, and desired effect, by priority, for PSYOP. Synchronize this element with the other IO elements.
      iii. Military deception (MILDEC). State how the military deception objectives and military deception tasks will deceive, and influence the enemy based on the approved COA. Synchronize this element with the other IO elements.
      iv. Electronic Warfare (EW). State how the EW objectives and EW tasks will degrade, disrupt, deny, and deceive the enemy based on the approved COA. State the defensive

and offensive EW measures. Identify target sets and effect, by priority, for EW operations. Synchronize this element with the other IO elements.

v. Information Assurance (IA). State how the IA objectives and IA tasks will deny the enemy access to our C4 based on the approved COA. Identify the information and INFOSYS for protection. Synchronize this element with the other IO elements.

vi. Counterdeception. State how the counterdeception objectives and counterdeception tasks will disrupt, deny and exploit the enemy based on the approved COA. Identify the units for protection. Synchronize this element with the other IO elements. Refer to Annex B, Intelligence, for detailed counterdeception information.

vii. Counterintelligence. State how the counterintelligence objectives and counterintelligence tasks will degrade, disrupt, deny and exploit the enemy based on the approved COA. Identify the units for protection. Synchronize this element with the other IO elements. Refer to Annex B, Intelligence, for detailed counterintelligence information.

viii. Counter propaganda. State how the counter propaganda objectives and counter propaganda tasks will degrade, disrupt, deny and exploit the enemy based on the approved COA. Identify the units for protection. Synchronize this element with the other IO elements.

ix. Physical destruction. State how the physical destruction objectives and physical destruction tasks will destroy, degrade, disrupt, and deny the enemy based on the approved COA. Identify target sets and effect, by priority, for destruction. Synchronize this element with the other IO elements.

x. Computer Network Operations (CNO). State how the CNO objectives and CNO tasks will destroy, degrade, disrupt, and deny the enemy based on the approved COA. Identify target sets and effect, by priority, for attack. Synchronize this element with the other IO elements.

xi. Physical Security. State how the physical security objectives and physical security tasks will deny the enemy based on the approved COA. Synchronize this element with the other IO elements.

xii. Special Information Operations. SIO may be classified. Access is restricted to strict need to know. Synchronize this element with the other IO elements.

xiii. Civil Affairs (CA). CA is a related activity to IO. State the IO objectives for CA.

xiv. Public Affairs (PA). PA is a related activity to IO. State the IO objectives for PA.

g. Describe the Perceptual Layers of IO:

i. Psychological: The psychological layer is aimed at management of the perception of a target audience.

ii. Information Infrastructure: This layer accepts processes, manages, and stores the information.

iii. Physical Layer: The final layer is the physical system level, which includes the computers, physical networks, telecommunications and supporting structure components that implement the information system.

5. **Intelligence Preparation**.

a. **Defensive IO and Information Assurance**. The CTF IOWG needs to know threat IO attack capabilities (if any) to facilitate defensive and information assurance programs. It is imperative that the CTF IOWG submits intelligence requirements as early as possible after CTF establishment. Potential intelligence requirements are as follows:

(1) Identify and monitor threat IO capabilities to influence CTF decision-making processes.
(2) Assess intent, and characterize their potential employment against the CTF.
(3) Determine threat IO actions to degrade, deny, or destroy CTF information systems.
(4) Identify IO actions against the CTF from any other source. Identify the originator, assess the threat, and monitor other potential avenues of attack for indications of a broader IO campaign (e.g. a concurrent press campaign, denial and deception, etc.). The level of perceived threat from a particular country or non-state entity will establish the intelligence priority.
(5) Determine which local, national, and international media are providing information to the populace.

(6) Determine local capabilities (print, radio, TV, methods of acquiring and transferring data) and identify vulnerabilities and threats to the flow of information.

b. **Offensive IO**. Intelligence is required to support planning and control of operations for offensive IO to include efforts to shape and influence perceptions, computer network attack or other courses of action taken against threats. Must define campaign objectives for IO attacks; monitor, coordinate, and integrate component activities to identify objectives and objective access; assess the objective's vulnerabilities and select the optimum IO attack. Potential intelligence requirements are as follows:

(1) Determine threat decision-making processes, associated personnel and organizations, and how they may be influenced. Develop detailed biographies on personnel involved and identify human factors that may influence their decision process.
(2) Identify national level military issues and social factors (political, economic, societal, and cultural), including interaction between political and military organizations and their decision-makers, and military Courses of Action (COAs).
(3) Identify communication methods to include, but not limited to: flow of information, links, nodes, systems, media, and other interactions. Develop capabilities that will allow access and ability to influence processes to support command IO objectives.
(4) Determine the objective's level of IO awareness, to include technical capabilities, IO technical associations (people, organizations, governments), and available hardware and software. Determine means to facilitate influencing these areas.
(5) Determine which local, national, and international media are providing information to the populace.
(6) Determine local capabilities (print, radio, TV, methods of acquiring and transferring data) and identify vulnerabilities and threats to the flow of information.

c. IO in the CCTF can be accomplished by Influence and/or Electronic approaches. The planning process should review and consider a combination of both Information Influence and the Information Environment. Planning should include, but is not limited to the following:

(1) Information Management. The objective of each of these actions is to refine the information processes to optimize the exploitation of available data and distribution of knowledge to appropriate users. The four categories of the IM for MPAT to support IO must include:
   a. Acquire the Right Data: The type, quality, accuracy, timeliness, and rate of data collected have a significant impact on knowledge delivered.
   b. Optimize the Extraction of Knowledge: The process of transforming data into knowledge may be enhanced or refined to improve efficiency, throughput, end-to-end speed, or knowledge yield.
   c. Distribute and Apply the Knowledge: The products of information process must be delivered to users on time, in understandable formats, and in sufficient quantity to provide useful comprehension to permit actions to be taken.
   d. Ensure the Protection of Information: In the competitive and conflict environments, information and the collection, processing, and distribution channels must be protected from all forms of attack to secure reliability for and availability to the user.
(2) Information Environment. The Information Environment (IE) is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. The five crucial dimensions for measuring the quality of information available within the CCTF are:
   a. Completeness: Are all the relevant items available, including entities, their attributes, and relationships between them.
   b. Correctness: Are all the items in the system faithful representations of the realities they describe.
   c. Currency: Age of the items of information, often termed their latency.
   d. Accuracy or Level of Precision: Which is conditional on the purpose the user has in mind.
   e. Consistency: Across different command centers, functionally specialized areas, and applications.

6. **Develop IO Measures of Effectiveness (MOE).** IO MOE are criteria established to aid in determining when the CTF commanders' IO objectives have been met.

a. Example MOEs:

(1) Level of public cooperation.
(2) Number of attacks against CTF Forces.

b. The following sources may contain information that can assist in determining MOE status.

(1) CTF intelligence updates.
(2) Commander's Feedback.
(3) Intelligence Reports.
(4) Media.
(5) Public Affairs Information.
(6) NGOs.
(7) Human sources.
(8) Information Operation Systems and Sources.
(9) Battle Damage Assessment

7. **IO Planning Guidance**. This guidance directs the development of IO and the associated delivery methods needed to achieve defined goals against specified objectives. Outlined below is the key planning principles and the IO Core Capabilities planning guidance summaries.

a. **Key Principles.** The following are key principles for planning, coordinating, and executing IO and should be used as appropriate for IO planning:

(1) Speak with one voice
(2) Know the target audience
(3) Focus on what is important
(4) Do not raise unattainable expectations
(5) Build upon the truth
(6) Centralized control; decentralized execution
(7) Use multiple means to convey information
(8) Synchronize efforts
(9) Strive to win local popular support

b. **Electronic Warfare (EW):** Actions involving the use of the electromagnetic spectrum to benefit CTF objectives. The CTF EW Officer working with CTF IO Chief will establish the process by which the CTF will coordinate and integrate the three aspects of Electronic Warfare [Electronic Warfare Support (ES), Electronic Attack (EA), and Electronic Protection (EP)].

(1) Electronic Warfare Support (ES). The CTF IO Cell in coordination with Intelligence (C2) and Operations (C3) must establish the CTF Intelligence Surveillance and Reconnaissance (ISR) tasking process and develop internal procedures for nominating objectives to that process for ISR collection.
(2) Electronic Attack (EA). The CTF EW Officer must establish how the CTF will coordinate and integrate jamming events. Normally, a Jamming Control Authority (JCA) will be assigned.
(3) Electronic Protection (EP). The CTF EW Officer must coordinate with Communications (C6) to establish how the CTF will conduct Frequency Management.
(4) See this Chapter C3, Annex D, Appendix 5, MNF SOP Additional Planning Guidance: The guidance relates to the development of EW from an IO perspective.

c. **Computer Network Operations (CNO).** IO involves measures that protect, defend, or attack information and information systems. CNO includes:

(1) Computer Network Attack (CNA),
(2) Computer Network Defense (CND), See this Chapter C3, Annex D, Appendix 7.
(3) Computer Network Exploitation (CNE).

d. **Operations Security (OPSEC):** A process of identifying friendly critical information and subsequently analyzing friendly actions attendant to military operations. Also included are activities

to identify actions observable by a threat to determine indicators that may be useful to the threat in a time sensitive manner. Ensure OPSEC efforts are considered when PAO, MILDEC, and PSYOPS are being conducted.

(1) The OPSEC assessment is a five-step process:
  (a) Identify unit or operation-specific critical information.
  (b) Define relevant threats.
  (c) Identify vulnerabilities.
  (d) Assess risk.
  (e) Select and implement OPSEC measures.

(2) Establish a list of Essential Elements of Friendly Information (EEFI).
(3) Request via the Supported Strategic Commander, a threat assessment of the objective of interest from the appropriate national support agencies in support of the CTF.
(4) Request national coalition interagency OPSEC support staffs, as appropriate, to study and identify critical information and EEFI associated with the operation.
(5) Protect Commander's Critical Information Requirements (CCIR) in classified message to all component and supporting commands.
(6) Request, via the Supported Strategic Commander, a collection on all friendly force components and supporting activities for the duration of the operation. Establish reporting criteria for feedback to ensure that OPSEC vulnerabilities are reported back to the CTF. Request immediate reporting for time sensitive support.
(7) Activate communications security monitoring support as early as possible to provide an early awareness of OPSEC vulnerabilities.
(8) Coordinate, with Operations, a process for disseminating any compromise or potential compromise in communications security to enhance operational awareness.
(9) See Chapter C3, Annex D, Appendix 6, MNF SOP Additional Planning Guidance: The guidance relates to the development of OPSEC.

e. **Military Deception (MILDEC).** Those measures designed to mislead an adversary/threat via manipulation, distortion, or falsification to induce the adversary/threat to react in a manner beneficial to CTF. NOTE: MILDEC may be a very close hold planning action that only a select group of CTF planners are involved with. This is because some or a major part of the CTF operational plan may, in fact, be essential parts of the deception plan. The fewer the personnel involved in MILDEC the more likely it will truly be deceptive in nature.

(1) Deception Mission Analysis. Deception mission analysis is conducted as part of the overall mission analysis.
(2) Deception Planning Guidance. After completion of the mission analysis, the commander issues planning guidance to the staff. In addition to other guidance, the commander states the deception objective for the operation. The commander may go on to provide additional guidance concerning specific deception COAs that the staff should address when preparing estimates.
(3) Staff Deception Estimate as part of the operations estimate. Working with the operational planners and intelligence analysts, the deception planners gather and analyze information relating to the threat. They identify the key decision makers and study all available information relating to their backgrounds and psychological profiles. They consider the threat's C2 system and decision-making process. They study its intelligence collection and analysis capabilities.
(4) See Chapter C3, Annex D, Appendix 4, MNF SOP Additional Planning Guidance, Military Deception: The guidance relates to the development of Military Deception (MILDEC) from an IO perspective.

f. **Psychological Operations (PSYOPS).** Planned operations to convey selected information and indicators to adversary/threat and/or neutral audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of the adversary/threat governments, organizations, groups, or individuals. The purpose of PSYOPS is to induce or reinforce adversary/threat attitudes and behavior favorable to CTF's Commanders objectives.

(1) PSYOPS messages. Initially, the PSYOPS Officer may not have approved PSYOPS products that are ready for delivery, which may delay start of influence operations. PSYOPS theme

approval for new messages and themes resides with the Lead Nation's national authorities unless delegated to the Supported Strategic Commander. The PSYOPS Officer develops themes in support of the CTF, and will advise the IOWG on delivery methods. The IOWG, in coordination with the PSYOPS Officer, must determine the process by which new themes will be approved.

(2) PSYOPS theme coordination. The PSYOPS officer must coordinate PSYOPS themes with PAO and CMOC.

(3) See Chapter C3, Annex D, Appendix 2, MNF SOP PSYOPS Additional Planning Guidance: The guidance relates to the development of Psychological Operations.

g. **Public Affairs (PA).** While it is important to remember that Public Affairs cannot be used to disseminate PSYOPS themes that are intended to deceive the recipient, Public Affairs is an excellent delivery tool to promote the Commanders information objectives. Close care must be taken not to violate the legal constraints placed upon Public Affairs Officers. See Chapter C3, Annex D, Appendix 3, MNF SOP Additional Planning Guidance, Public Affairs. The guidance relates to the development of PA from an IO perspective.

D. Responsibilities. CTF IO. The CTF C3 has overall responsibility for planning and execution of CTF IO, which is published in the CTF OPORD IO Annex. The CTF IO Chief is responsible to CTF C3 for all CTF IO planning and integration and heads both the CTF IO Cell and CTF IOWG. CTF IO Cell and CTF IOWG membership will vary based upon the CTF mission and headquarters composition. Typical membership includes the following positions:

1. CTF IO Chief

a. Directs and coordinates IO cell and IOWG efforts.
b. Provides an IO watch officer to the Coalition / Combined Operations Center (COC).
c. Provides an IO representative to C5 Plans and C3 FOPS.
d. Coordinates all CTF IO efforts with CTF components and Supported Strategic Commander's staff.
e. Serves as Liaison Officer to Coalition / Combined Targeting Coordination Board (CTCB).
f. Coordinates IO intelligence requirements through the C2.
g. Capable of working at the highest levels of CTF classification.
h. Have complete access to the deception plan in order to enhance his ability to coordinate the deception plan with other elements of IO.

2. CTF IO Deputy Chief

a. Responsible for CTF IO while CTF IO Chief is engaged with meetings, working groups, and other duties.
b. Usually serves as IO representative to C5 Plans ensuring integration of IO.
c. Capable of working at the highest levels of CTF classification.

3. Information Operations Watch Officer

a. Serves as central point of contact for IO within the COC watch.
b. Maintains log of significant events and pending actions.
c. Ensures appropriate C3 IO Cell and/or IOWG members are advised of higher HQs tasking.
d. Keeps COC Chief informed of IO activities.
e. Monitors events and provides recommendations for IO support to the CTF.
f. Submits and tracks IO Requests for Information (RFI).

4. CTF Operations Security (OPSEC) Officer

a. Develops and updates the OPSEC plan as part of the CTF OPORD, to include:

(1) Identification of Essential Elements of Friendly Information (EEFI).
(2) Analysis of threats to critical information.
(3) Analysis of OPSEC vulnerabilities to identify tentative OPSEC measures.
(4) Assessment of risk to determine which OPSEC measures to employ.
(5) Application of appropriate countermeasures.

b. Initiates a feedback program. Monitoring tasks include intelligence and counter-intelligence collection, examination of public media, and reporting of OPSEC measures implemented.
c. Coordinates all OPSEC activities with other facets of the CTF plan.
d. Coordinates and reports on COMSEC Monitoring Activities.
e. Provides information on COMSEC efforts and recommends CTF Information Management (IM) plan adjustments to the CTF IM and C6.

5. CTF Deception Officer

a. Coordinates development and update of the deception element of the CTF plan with staff members and component representatives on a strict need to know basis. The basis for deception objectives is often related to OPSEC objectives.
b. Monitors dissemination of deception related information in accordance with CTF guidance. This will normally include at least two levels of access with only a relatively small number of people having access to the entire deception plan.
c. Coordinates, normally via the CTF IO Chief, with PSYOPS, PA, OPSEC, EW, and intelligence.
d. Coordinates with C2 Intelligence for collection management coverage in support of deception planning and operations.
e. Monitors execution of the deception plan.

6. CTF Electronic Warfare (EW) Officer

a. Prepares CTF EW elements (EA, ES, and EP) of CTF OPORD).
b. Coordinates with Coalition / Combined Frequency Management Center (CFMC).
c. Coordinates with CTF C6 Coalition / Combined Frequency Management Element (CFME).
d. Provides frequency management monitoring and advice to CTF IO Cell and CTF IOWG.

7. CTF PSYOPS Officer

a. Coordinates with the Supported Strategic Commander for PSYOPS guidance for CTF input and national or multinational forces' themes with Lead Nation national authorities, Supporting national authorities, and nations' interagency processes.
b. Integrates and coordinates all aspects of CTF PSYOPS with CTF IO Cell and CTF IOWG.

8. Computer Network Operations (CNO) Officer

a. Provides CNA, CNE and CND planning support to CTF IO Cell and CTF IOWG.
b. Coordinates with the Supported Strategic Commander for approval and execution of CNO.
c. Coordinates with CTF C6 to assess intrusions and attacks.
d. Provides ability to draw upon the capabilities of other coalition military organizations and governments or non-government agencies insights.
e. Recommends changes to the CTF network security posture.
f. Coordinates with CTF C6 to conduct risk assessment of the CTF network security posture.
g. Higher security clearance capable.

9. Intelligence representative

a. Provides timely and directed intelligence support to CTF IO Cell and CTF IOWG.
b. Provide inputs for Battle Damage Assessments (BDA) / Measures of Effectiveness (MOE) and effects feedback for IO initiatives as reflected in the CTF OPORD or Campaign Plan.
c. Assists in the development of IO High Priority Targets (HPT) and/or audiences.
d. Provides input on IO threat, capabilities, and estimates to include Electronic Order of Battle, threat Tactics, Techniques, and Procedures (TTP), and threat commander profiles, etc.
e. Assists in identifying IO indicators and warning (I&W).
f. Provides input on counter-intelligence situational awareness to the CTF IO Cell and CTF IOWG.
g. Attends the Intelligence Collection and Synchronization Board (ICSB) or equivalent.

10. Logistics representative

a. Integrates IO considerations and objectives into the logistics planning process.
b. Provides subject matter expertise to the CTF IOWG.
c. Ensure host nation and NGO / International Organization requirements are identified prior to CTF arrival (if possible).

11. Communications representative (see Chapter C-6 for additional information)

    a. Provide expertise on CTF Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) architecture and critical nodes.
    b. Provides Coalition / Combined Restricted Frequency List (CRFL) input to the frequency management effort.
    c. Provides information systems impact for Emission Control (EMCON) and network security.

12. Public Affairs Officer

    a. Advises on timely dissemination of accurate information in response to propaganda.
    b. Coordinates command information program with CTF IOWG.
    c. Coordinates PA communication points with PSYOPS themes.
    d. Provides feedback/analysis on CTF IO effectiveness with respect to objective media.
    e. Ensures all publicly releasable information is screened for OPSEC.

13. Legal Officer

    a. Provides legal guidance and planning assistance to CTF IOWG.
    b. Assists CTF IOWG with interagency coordination and negotiations.

14. Civil Affairs (CA) representative

    a. Ensures the consistency of civil military operations within the CTF AO.
    b. Coordinates CMO activities with the CTF IOWG in support of IO related objectives.
    c. Provides feedback/analysis on CTF IO effectiveness with respect to objective leadership and civilian populace, IOs and NGOs in the CTF AO.

15. Force Protection LNO. Represents the CTF IOWG in CTF Force Protection planning

16. IO representation to C5 Plans and C3 FOPS. IO representatives must liaison with the C5 Plans Working group and the C3 FOPS working group to ensure appropriate consideration and integration of IO capabilities in future plans.

E. Considerations

1. It is imperative that IO initiatives are coordinated and approved as early as possible when the CTF is activated. Various IO products, such as CNA and PSYOPS, require approval at the Lead Nation, supporting nations and/or at strategic levels.
2. Conducting Combined/Coalition Information Operations can present classification challenges that must be addressed during combined planning. Use of the Coalition Coordination Center (CCC) can greatly assist in this process.
3. Upon standing up the CTF, identify early on communications connectivity requirements for support to the IO Cell and IOWG.

4. The specific manning requirements and number of augmentees to the IO Cell and CTF IOWG should be tailored to meet mission requirements identified in Crisis Action Planning and CCTF's guidance.

F. Reports and Products

1. OPSEC/COMSEC critical disclosure report. This is a near real time voice report (followed by a hard copy report) from the communications security monitoring support team to the CTF IO Chief to report a serious OPSEC/COMSEC disclosure.
2. OPSEC/COMSEC disclosure daily summary report. This is a report from the communications security monitoring support team to the CTF IO Chief recording significant OPSEC/COMSEC disclosures for the previous 24 hours.
3. Network Vulnerability Change Implementation Status Reports. This is a communication from the CCTF to the Supported Strategic Commander C6. This communication reports compliance with directed changes to network hardware, software, processes, or procedures to improve overall security of the CTF network
4. Network Security Posture Change/Attainment Messages. This is either a message from the CCTF to CTF components to direct a change, or from the CCTF to the Supported Strategic Commander to report attainment (or request waiver).
5. Input to the Commander's Daily Guidance and/or Situational Report to the Supported Strategic Commander (SITREP). The CTF IO Cell (IO Watch Officer) will provide any significant IO activities to the Operations Division for inclusion in the Commander's Daily Guidance and/or SITREP
6. CTF Courses of Action (COA) Matrix. A matrix used by the CTF staff, which contains IO capabilities, mapped against themes and objectives, which delineate specific tasks required to support each theme. This Matrix needs to be closely coordinated with the Supported Strategic Commander within the MNF effort. In some situations, the Supported Strategic Commander will be heavily involved in IO planning and operational execution. In other CTF scenarios, the Supported Strategic Commander will have limited IO planning and operational execution responsibilities. In either case, the COA Matrix is a useful vehicle for CTF coordination.
7. CTF IO Synchronization Matrix. The CTF IOWG develops and maintains a coordination matrix similar to the one shown below (Fig. C-3-D-1) depicting the IO events occurring through each phase of the operation overlaid upon the CTF IO areas and CTF Components. This matrix provides a visual display of the CTF actions and helps to readily de-conflict IO actions with other operations.

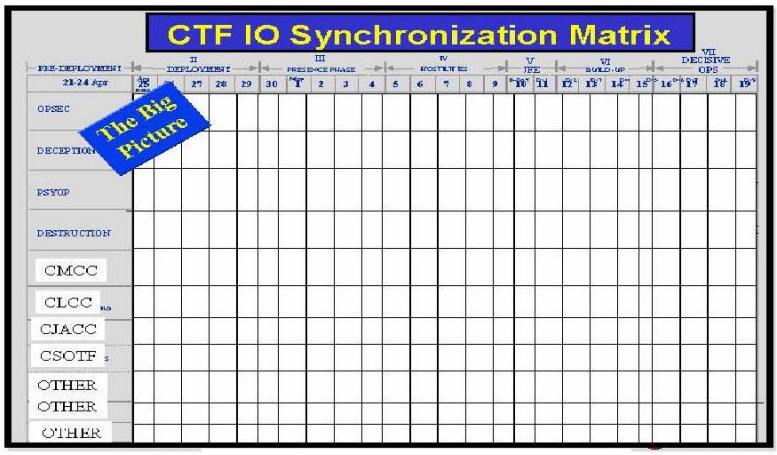

Figure: C3-D-2 CTF IO Synchronization Matrix

8. Daily Press Analysis Report. Analysis provided by the PA representative to the CTF IO Cell of international, regional, and local media reporting of CTF mission and operations.
9. Daily IO Log. Created and maintained (on a 24 hour basis) by the CTF IO Cell to record all relevant IO events, documents and requirements to ensure continuity of information for the CTF IO organization.

G. References

1. U.S. Joint Publication 3-13, Joint Doctrine for Information Operations.
2. U.S. Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W) Operations.
3. U.S. Joint Publication 3-51, Electronic Warfare in Joint Military Operations.
4. U.S. Joint Publication 3-53, Doctrine for Joint Psychological Operations.
5. U.S. Joint Publication 3-54, Joint Doctrine for Operations Security.
6. U.S. Joint Publication 3-58, Joint Doctrine for Military Deception.

H. Appendixes

1. Appendix 1, ADDITIONAL GENERAL PLANNING GUIDANCE
2. Appendix 2, ADDITIONAL PLANNING GUIDANCE, PSYOPS
3. Appendix 3, ADDITIONAL PLANNING GUIDANCE, PUBLIC AFFAIRS
4. Appendix 4, ADDITIONAL PLANNING GUIDANCE, MILITARY DECEPTION
5. Appendix 5, ADDITIONAL PLANNING GUIDANCE, ELECTRONIC WARFARE
6. Appendix 6, ADDITIONAL PLANNING GUIDANCE, OPERATIONS SECURITY
7. Appendix 7, ADDITIONAL PLANNING GUIDANCE, DEFENSIVE INFORMATION OPERATIONS
8. Appendix 8, OFFENSIVE AND DEFENSIVE IO TASK SELECTION MATRIX

Appendix 1

ADDITIONAL GENERAL PLANNING GUIDANCE

Annex D INFORMATION OPERATIONS

Chapter C-3 OPERATIONS

A. Situation

1. **Threat**
   a. What are the threat situations, force dispositions, intelligence capabilities, and possible threat COAs?
   b. Is there any specific information that bears directly on the planned IO?
2. **Friendly**
   a. What is the situation of friendly forces that may directly affect attainment of IO objectives?
   b. Are there any critical limitations and other conflicting planned IO activities?
3. **Assumptions**
   a. What are the assumptions concerning friendly, threat, or third-party capabilities, limitations, or COAs?
   b. What conditions does the commander believe will exist when the plan becomes an order?

B. Mission. What is the IO mission (who, what, when, where, why)?

C. Execution

1. **Concept of Operations**
   a. How does the commander visualize the execution of IO from beginning to termination?
   b. How will IO support the commander's mission? What are the concepts for supervising and terminating IO?
2. **IO Tasks**
   a. What are the major tasks for military deception? (See ADDITIONAL PLANNING GUIDANCE, MILITARY DECEPTION)
   b. What are the major tasks for EW? (See ADDITIONAL PLANNING GUIDANCE, ELECTRONIC WARFARE)
   c. What are the major tasks for OPSEC? (See ADDITIONAL PLANNING GUIDANCE, OPERATIONS SECURITY)
   d. What are the major tasks for PSYOPS? (See ADDITIONAL PLANNING GUIDANCE, PSYOPS)
   e. What are the major tasks for physical destruction related to IO?
   f. What are the major tasks for PA? (See ADDITIONAL PLANNING GUIDANCE, PUBLIC AFFAIRS)
   g. What are the major tasks for Civil Affairs?
3. **Coordinating Instructions.** What, if any, are the mutual support issues relating to the elements of IO?

D. Administrative and Logistics

1. What are the administrative requirements related to IO?
2. What are the logistics requirements related to IO?

E. Command and Control

1. What are the C2 instructions related to IO?
2. What is the command structure for IO? Are there any special communications and reporting requirements for IO? If so, what are they?

Appendix 2

ADDITIONAL PLANNING GUIDANCE, PSYOPS

Annex D INFORMATION OPERATIONS

Chapter C-3 OPERATIONS

A. Situation

1. **Overview**
   a. What is the general psychological situation in the AO?
      1. Each type of PSYOP is categorized into strategic, operational, or tactical level psychological operations.
      2. Strategic level PYSOP: is conducting international information activities to influence foreign attitudes, perceptions, and behavior in favor of US goals and objectives.
      3. Operational level PYSOP: activities are designed to strengthen US and multinational capabilities to conduct military operations in the operational area and accomplish particular missions across the range of military operations.
      4. Tactical level PSYOP: are outline how military force will be employed against opposing forces to attain tactical objectives
   b. What, if any, are the ongoing PSYOPS programs?
   c. What are the significant factors influencing PSYOPS activities?
   d. What are the competing PSYOPS goals in the AO?
   e. What is the PSYOPS task to be accomplished?

2. **CTF Perspective**
   a. How will the assigned PSYOPS task be accomplished?
   b. What resources will be used?
   c. What will be the general phasing of current actions with future actions?

3. **Neutral Perspective** (if applicable)
   a. What are the estimated neutral intentions under various circumstances?
   b. What activities and resources are available to these neutral intentions?
   c. What neutral actions and behavior would favor mission accomplishment?
   d. Which apparent current COAs might affect mission accomplishment?
   e. What resources are available to execute alternative COAs?
   f. What objective and subjective factors could affect decisions and resource effectiveness?
   g. What are the staff factions and who are the particularly influential individuals?
   h. What are the characteristics of decision makers and their key advisors, major staff planners, staff factions (to include particularly influential individuals), and intelligence system analysts?
   i. What are the groups of related planner and decision maker essential elements of friendly information (EEFI)?
   j. What is the estimated background knowledge and desired and harmful appreciations for each group?

4. **Threat Perspectives**

   a. **Decision Maker and Staff**
      (1) Who are the decision makers who can direct development or allocation of resources of COA pertinent to the task assigned?
      (2) What feasible alternative actions would favor or harm friendly operational effectiveness?
      (3) What COAs might affect friendly task accomplishment?
      (4) What resources are available to execute each COA?
      (5) What are the characteristics of threat decision makers, their key advisors, and staff (particularly intelligence analysts) and their intent?

   b. **Intelligence Systems**
      (1) What are the intelligence systems that support decision makers and their staffs?

(2) What are the intelligence systems' capabilities pertinent to the situation?
(3) What are the objective and subjective factors and the characteristics of collection planners and decision makers that affect their development and selection for use of information gathering resources?
(4) What are the groups of related planner and decision maker EEFI?
(5) What is the estimated background knowledge and desired and harmful appreciations for each group?

c. **Audiences**
(1) What groups can influence plans, decisions, and operational effectiveness in task accomplishment?
(2) How susceptible are these groups to PSYOPS?
(3) What group behavior is favorable or harmful to task accomplishment?
(4) What are the apparent goals, motivations, and characteristics of each group?
(5) Who are the leaders who can cause these groups to behave in various ways?
(6) What are the groups of related target audience EEFI?
(7) What is the estimated background knowledge and desired and harmful appreciations for each group?

d. **Command Systems**
(1) What communications systems and command centers will be used to plan COAs and control, coordinate, and supervise execution of the planned COA?
(2) What is the purpose and what are the characteristics of each command and control communications net?
(3) What are the PSYOPS targets for jamming or attacking?
(4) When should PSYOPS be used to demoralize and disorganize the threat?
(5) When should PSYOPS be used to reduce threat operational effectiveness?
(6) When should PSYOPS be used to enhance the effectiveness of planned deceptions and PSYOPS?
(7) When should PSYOPS be used to support OPSEC to the maximum advantage?

B. Mission. How will the PSYOPS mission support the maneuver commander?

C. Execution

1. **Concept of Operations**
a. **Overview**
(1) What is the commander's intent?
(2) What is the overall concept for using PSYOPS in support of task accomplishment?
(3) Who will plan and conduct strategic PSYOPS in peacetime and in support of pre-conflict deterrence options? Who are the supporting commanders?
(4) Who will plan and conduct strategic and theater PSYOPS in support of sustained conflict? Who are the supporting commanders?
(5) Who will plan and conduct joint tactical PSYOPS in support of operational COAs? Who are the supporting commanders?

b. **General Guidance to CTF**
(1) What are the valid PSYOPS themes to be promoted to induce strategic and theater PSYOPS objectives?
(2) What are the valid or invalid PSYOPS themes to be discouraged? Include indications of specific audience sensitivities and harm that might occur if the audiences accept the themes.
(3) PSYOPS actions suitable for use.
(a) What is the guidance for the conduct of military operations, actions, and personnel behavior to promote valid PSYOPS themes?
(b) What is the guidance for avoiding military operations and actions and personnel behavior that would result in harmful audience attitudes and behavior?
(c) What are the cultural and psychological characteristics of audiences that will aid operational planners and personnel in selecting COAs and interacting with audience members?
(4) Threat PSYOPS

(a) What threat PSYOPS will be directed at coalition personnel and at friendly foreign groups in the AO.
(b) What is the guidance for countering such threat operations?

c. **Outline of Each Planned PSYOPS Operation**
(1) What is the audience and set of PSYOPS objectives, overall themes, subgroups to be influenced (to include their characteristics), and specific themes to be promoted for each subgroup?
(2) What are the provisions for testing, producing, stocking, and disseminating PSYOPS materials and for measuring PSYOPS effectiveness?
(3) What are the command and staff arrangements?
(4) Who are the supporting commanders?
(5) What resources are required to plan and conduct PSYOPS actions? Include civil capabilities; indigenous assets; exploitation of threat detainees and other internees for PSYOPS; and military PSYOPS resources.
(6) What are the logistics requirements? Include preparation, distribution, and stocking of PSYOPS materials; transport of PSYOPS material and personnel to operational areas and their basing and support while conducting PSYOPS; provisions for the supply and maintenance of coalition and indigenous PSYOPS material; and fiscal and personnel matters.
(7) What are the requirements for implementing schedules and PSYOPS operation control sheets?
(8) What is the codeword for OPSEC sensitive PSYOPS?
(9) What is the OPSEC planning guidance? Include planning for, preparing for, and conducting PSYOPS and PSYOPS actions to maintain essential secrecy for the commander's intention and to gain and maintain essential secrecy for OPSEC sensitive PSYOPS COAs.

2. **Situation Monitoring**
a. How will intelligence, multi-discipline CI (MDCI), security monitoring, and operational feedback be provided?
b. What is the requirement for running situation estimates; periodic estimates of audience appreciations responsive to EEFI, actions, and attitudes and behavior; and current reporting of intelligence and multi-discipline CI information, security monitoring results, and implementing actions?
c. What resources are required? What is their availability?

3. **Control**
a. How will control be effected and implementation centrally coordinated?
b. What are the coordinating instructions?
c. How will implementation planning and supervision of the planned action be accomplished?
d. What is the need for specific PSYOPS operations?
e. What coordination is required with adjacent commands and civilian agencies, to include diplomatic missions and other agencies?
f. What coordination is required with military deception and OPSEC planners, EW planners, and planners in the fields of civic action, HA, civil affairs, CI, detainees, internees, command, control, and communications, legal, and operations?

4. **Tasks**
a. What responsibilities must be assigned to implement the concept?
b. Is designation of an executive agent to coordinate implementation among multiple organizations required?
c. How will feedback to ensure effectiveness of tasks be provided?

D. Administrative and Logistics

1. **Administrative**
a. What are the requirements for special reports?
b. What are the requirements for planning and operations in support of education programs regarding detainees and civilian internees?
c. What will be the participation in interrogation of internees and detainees to obtain information essential or peculiar to PSYOPS?

2. **Logistics**
   a. What is the guidance on stocking of PSYOPS and information materials and provisions to disseminating organizations?
   b. What are the provisions for the supply and maintenance of PSYOPS-unique supplies and equipment?
   c. What are the provisions for control and maintenance of indigenous equipment and materials?
   d. What are the fiscal matters relating to special funds?
   e. What are the personnel matters relating to indigenous personnel?

E. Command and Control

1. What are the recognition and identification instructions?
2. What is the electronic policy?
3. What are the headquarters locations and movements?
4. What are the code words?
5. What is the frequency allocation?

Appendix 3

ADDITIONAL PLANNING GUIDANCE, PUBLIC AFFAIRS

Annex D INFORMATION OPERATIONS

Chapter C-3 OPERATIONS

A. Situation

1. **General.** What are the general responsibilities and guidance for military PA actions (public information/media relations, command and internal information, and community relations)?
2. **Threat.** What are the expected actions of threat forces and forces hostile to coalition interests?
3. **Friendly.** What are the friendly agencies not under CCTF control that will contribute to the PA effort?
4. **Policy.** What is the applicable PA policy pertaining to this plan?
5. **Assumptions**
   a. What are the host-nation preferences and/or sensitivities to be considered in developing and executing PA programs?
   b. Should the CCTF be prepared to host the National Media Pool during the initial stages of operations?

B. Mission. What are the tasks and purposes of PA in the operation?

C. Execution

1. **Concept of Operations.** What PA support will be required in the following five phases.
   a. Precrisis
   b. Lodgment
   c. Decisive action and stabilization
   d. Follow-through
   e. Post-crisis, including redeployment

2. **Tasks**
   a. What are the PA tasks to be completed during the above-listed phases?
   b. What, if any, are the additional information release instructions to the supported commander and other supporting commands, to include release authority and PA guidance on casualty and mortuary affairs, postal affairs, missing in action, and detainee and internee matters?
   c. What are PA visual information and combat camera requirements?
   d. What are the detailed personnel and equipment support requirements to MNF commands?
   e. What are other supporting commands' support requirements?

3. **Coordinating Instructions**
   a. **Command Relationships.** What are the PA command relationships?
   b. **Coordination of Release of Information.** What are the detailed procedures for all supporting commands for handling or forwarding to the supported command queries, responses, and proposed news releases for clearance?
   c. **Other Coordinating Instructions**
      (1) What is the guidance for interviews and news conferences with returned MNF personnel or detained personnel?
      (2) What is the required PA coordination with other staff elements involved in release of information outside the command?
      (3) What are the procedures for keeping PA historical records?

D. Registration. What is the guidance for accreditation of the media?

E. Security Review. What, if any, are the security review procedures?

F. Arrangements for the Media

Appendix 4

ADDITIONAL PLANNING GUIDANCE, MILITARY DECEPTION

Annex D INFORMATION OPERATIONS

Chapter C-3 OPERATIONS

A. Situation

1. **General.** What is the general overall situation concerning military deception?
2. **Threat.**
   a. **General Capabilities.** What are the threat military capabilities relating directly to the planned deception? Military deception are actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are:
      i. Strategic Military Deception: Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations.
      ii. Operational Military Deception: Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater to support campaigns and major operations.
      iii. Tactical Military Deception: Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements.
      iv. Service Military Deception: Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems.
      v. Military Deception in of OPSEC: Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities.
   b. **Deception Targets and or Audiences.** What are the deception objectives?
   c. **Objectives Biases and Predispositions.** What are the objective's biases and predispositions?
   d. **Probable Threat COA.** What is the probable threat COA?
3. **Friendly**
   a. What is the friendly forces situation?
   b. What are the critical limitations?
   c. What is the concept of friendly operations?
4. **Assumptions**
   a. What are the assumptions concerning friendly, threat, or third-party capabilities, limitations, or COAs?
   b. What are the conditions the commander believes will exist when the plan becomes an order?

B. Mission

1. **Operational Mission.** See paragraph 2 of the basic plan or order.
2. **Deception Mission**
   a. **Deception Goal.** What is the desired effect or end state the commander wishes to achieve?
   b. **Deception Objective(s).** What is the desired action or inaction by the threat at the critical time and location?
   c. **Desired Threat Perceptions.** What must the deception objective believe for them to make the decision that will achieve the deception objective?

d. **Deception Story.** What scenario will cause the deception objective to adopt the desired perception? Consider one of the COAs discarded during plan preparation.

C. Execution

1. **Concept of the Operation**
   a. **General.** What is the framework for the operation? Include a brief description of the phases of the deception operation.
   b. **Other IO Capabilities**
      (1) What other capabilities will be used to support the deception operation?
      (2) What are the other plans and operations pertinent to the deception?
      (3) What coordination and de-confliction is required?
   c. **Feedback and Monitoring**
      (1) What type of feedback is expected, if any, and how will it be collected?
      (2) What impact will the absence of feedback have on the plan?
   d. **Means.** By what means will the deception be implemented?
   e. **Tasks.** What are the execution and feedback tasks to organizations participating in the execution and monitoring of the deception?
   f. **Risks**
      (1) Deception is successful. What is the likely threat response? What will be the impact on friendly forces from threat intelligence sharing?
      (2) Deception fails. What is the impact if the deception objectives ignores the deception or fails in some way to take the actions intended?
      (3) Deception is compromised. What is the impact of such a compromise on friendly forces and attainment of friendly objectives?
2. **Coordinating Instructions**
   a. What are the tasks or instructions listed in the preceding subparagraphs pertaining to two or more units?
   b. What is the tentative execution time frame, if applicable, and any other information required to ensure coordinated action between two or more elements of the command?

D. Administrative and Logistics

1. **Administrative**
   a. **General.** What are the general procedures to be employed during planning, coordination, and implementation of deception activities?
   b. **Specific.** What, if any, are the special administrative measures required for the execution of the deception operation?
2. **Logistics.** What are the logistics requirements for the execution of the deception operation (transportation of special material, provision of printing equipment and materials)?
3. **Costs.** What are the applicable costs associated with the deception operation?

NOTE: Do not include those administrative, logistics, and medical actions or ploys that are an actual part of the deception operation.

E. Command, Control, and Communications

1. **Command Relationships**
   a. **Approval.** What is the approval authority for execution and termination?
   b. **Authority.** Who are the designated supported and supporting commanders and supporting agencies?
   c. **Oversight.** What are the oversight responsibilities, particularly for executions by non-organic units or organizations outside the chain of command?
   d. **Coordination**
      (1) What are the AO coordination responsibilities and requirements related to deception executions and execution feedback?
      (2) What are the other coordination responsibilities and requirements related to deception executions and execution feedback?
2. **Communications**

a. What are the communications means and procedures to be used by control personnel and participants in the deception operation?
b. What are the communications reporting requirements to be used by control personnel and participants in the deception operation?

F. Security

1. **General.** What are the general security procedures to be employed during planning, coordination, and implementation of deception activities?
2. **Specific**
   a. What are the access restrictions and handling instructions to the deception appendix or plan?
   b. Who has authority to grant access to the deception appendix or plan?
   c. How will cover stories, code words, and nicknames be used?
   d. How will planning and execution documents and access rosters be controlled and distributed?

Appendix 5

ADDITIONAL PLANNING GUIDANCE, ELECTRONIC WARFARE

Annex D INFORMATION OPERATIONS

Chapter C-3 OPERATIONS

A. Situation

1. **Threat Forces**
   a. What are the capabilities, limitations, and vulnerabilities of threat communications, non-emitting, and EW systems?
   b. What is the threat capability to interfere with accomplishment of the EW mission?
2. **Friendly Forces**
   a. What friendly EW facilities, resources, and organizations may affect EW planning by subordinate commanders?
   b. Who are the friendly forces with which subordinate commanders may operate?
3. **Assumptions.** What are the assumptions concerning friendly or threat capabilities and COAs that significantly influence the planning of EW operations?
4. **Additional Information on EW.**
   a. Electronic Attack (EA) is the division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).
   b. Electronic Protection (EP) is the division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.
   c. Electronic Warfare Support (ES) is the division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localizes sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. ES data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence.

B. Mission. What is the EW mission (who, what, when, where, why)?

C. Execution

1. **Concept of Operations**
   a. What is the role of EW in the commander's IO strategy?
   b. What is the scope of EW operations?
   c. What methods and resources will be employed? Include organic and non-organic capabilities?
   d. How will EW support the other elements of IO?
2. **Tasks.** What are the individual EW tasks and responsibilities for each component or subdivision of the force? Include all instructions unique to that component or subdivision.
3. **Coordinating Instructions**
   a. What instructions, if any, are applicable to two or more components or subdivisions?
   b. What are the requirements, if any, for the coordination of EW actions between subordinate elements?
   c. What is the guidance on the employment of each activity, special measure, or procedure that is to be used but is not covered elsewhere in this tab?
   d. What are the emissions control guidance?

e. What coordination with the C-6 is required to accomplish the JRFL?

D. Administrative and Logistics

1. **Administrative**
   a. What, if any, administrative guidance is required?
   b. What, if any, reports are required? Include example(s).
2. **Logistics.** What, if any, are the special instructions on logistic support for EW operations?

E. Command and Control

1. **Feedback**
   a. What is the concept for monitoring the effectiveness of EW operations during execution?
   b. What are specific intelligence requirements for feedback?
2. **After-Action Reports.** What are the requirements for after-action reporting?
3. **Signal.** What, if any, are the special or unusual EW-related communications requirements?

Appendix 6

ADDITIONAL PLANNING GUIDANCE, OPERATIONS SECURITY

Annex D INFORMATION OPERATIONS

Chapter C-3 OPERATIONS

A. Situation

1. **Threat Forces**
   a. **Current Threat Intelligence Assessment**
      (1) What is the estimated threat's assessment of friendly operations, capabilities, and intentions?
      (2) What is the known threat knowledge of the friendly operation addressed in the basic plan?

   b. **• Threat Intelligence Capabilities**
      (1) What are the threat's intelligence collection capabilities according to major categories (signals intelligence, HUMINT, imagery intelligence)?
      (2) What potential sources (including other nations) provide support to the threat?
      (3) How does the threat's intelligence system work? Include the time required for intelligence to reach key decision makers.
      (4) What are the major analytical organizations and who are the key personalities?
      (5) What, if any, unofficial intelligence organizations support the national leadership?
      (6) What are the threat intelligence capabilities strengths and weaknesses?

2. **Friendly Forces**
   a. **Friendly Operations.** What are the major actions to be conducted by friendly forces in the execution of the basic plan?
   b. **Critical Information.** What is the identified critical information? Include the critical information of higher headquarters. For phased operations, identify the critical information by phase.
   c. **Assumptions.** What are the assumptions upon which this OPSEC plan is based?

B. Mission. What is the OPSEC mission (who, what, when, where, why)?

C. Execution

1. **Concept of Operations**
   a. What is the role of OPSEC in the commander's IO strategy?
   b. What is the general concept for the implementation of planned OPSEC measures? Describe these by phase and major activity (maneuver, logistics, communications), if appropriate.
   c. What will be the OPSEC support to other capabilities or activities?
2. **Tasks.** What are the specific OPSEC measures to be executed? List these by phase and include specific responsibilities for subordinate elements.
3. **Coordinating Instructions**
   a. What are the requirements for coordination of OPSEC measures between subordinate elements?
   b. What is the required coordination with public affairs?
   c. What is the guidance on termination of OPSEC related activities?
   d. What is the guidance on declassification and public release of OPSEC related information?

D. Administrative and Logistics

1. What, if any, are the OPSEC related administrative or logistic support requirements?
2. What, if any, are the administrative or logistics related OPSEC measures?

E. Command and Control

1. **Feedback**
   a. What is the concept for monitoring the effectiveness of OPSEC measures during execution?

b. What are the specific intelligence requirements for feedback?

2. **OPSEC Surveys.** What are the plans for conducting OPSEC surveys in support of this operation?
3. **After-Action Reports.** What are the requirements for after-action reporting?
4. **Signal.** What, if any, are the special or unusual OPSEC-related communications requirements?

Appendix 7

ADDITIONAL PLANNING GUIDANCE, DEFENSIVE INFORMATION OPERATIONS

Annex D INFORMATION OPERATIONS

Chapter C-3 OPERATIONS

A. Situation

1. **General**
   a. What are the defensive IO objectives?
   b. How do these objectives relate to mission accomplishment?
2. **Threat.** What are the threat capabilities that affect friendly information, and information systems, and IO not already discussed in Annex K?
3. **Friendly.** What are the organizations that are not subordinate to this command and the specific tasks assigned to each supporting defensive IO objective?

B. Mission. How do defensive IO support the accomplishment of the mission assigned in the basic plan?

C. Execution

1. **Concept of Operations**

   a. **General.** What is the overall concept for ensuring friendly information access and availability despite threat IO use? Pay particular attention to physical security and survivability of friendly information system capabilities and facilities.
   b. **Phasing**
      (1) What are the defensive IO activities occurring in each operational phase? Describe activity sequences in each phase keyed to phase initiation and supported operational events.
      (2) What is the time-phased guidance for accomplishing actions implementing the defensive IO plan?

2. **Tasks**
   a. What command element is responsible for coordinating defensive IO actions?
   b. What are the assigned tasks and responsibilities of each subordinate command to implement and accomplish defensive IO actions, to include identification of vulnerabilities?

3. **Coordinating Instructions**

   a. **Integration**
      (1) What are the detailed instructions for accomplishing integration of physical security and survivability measures, electronic warfare, INFOSEC, CI, PA, counter-PSYOPS, counter-deception, and OPSEC means of performing defensive IO?
      (2) What is the guidance for mitigation and/or negation of threat capabilities?
   b. **Coordination.** What are the detailed requirements for coordinating among elements involved in defensive IO? Emphasize close coordination with IO, C2W, deception, OPSEC, EW, PSYOPS, intelligence, PA, and other key planners that rely on friendly information resources.
   c. **Security.** What, if any, are the special security or handling requirements for defensive IO planning and actions envisaged by this appendix?
   d. **Reports.** What, if any, are the operational reporting requirements necessary for effective monitoring of defensive IO activities?

D. Administrative and Logistics

1. **Personnel.** What, if any, are the requirements for specialized personnel qualifications and/or qualification?

2. **Supply.** What, if any, are the specialized equipment supply requirements?
3. **Reports.** What, if any, are the required administrative reports?

E. Command and Control. What special systems or procedures, if any, are required for C2 of defensive IO actions?

Appendix 7

OFFENSIVE AND DEFENSIVE IO TASK SELECTION

Annex D INFORMATION OPERATIONS

APPENDIX B: OFFENSIVE AND DEFENSIVE IO TASK SELECTION

FORM 1: Identify the IO Objectives by review/identify CCTF objectives:

FORM 2: Identify Specified, Implied and subsidiary tasks associated with the CC objectives:

1) Specified task:
2) Implied task:
3) Subsidiary tasks:

FORM 3: Evaluate the Specified, Implied and subsidiary tasks.

1) Specified task:
2) Implied task:
3) Subsidiary Tasks:

FORM 4: Evaluate tasks according to the criteria.

	Capability (.25)			Constraints (.25)			Feasibility (.25)				Vulnerability (.25)		Total
Tasks	Efficiency	Success	Total	Political	ROE	Culture	Total	Technical	Resource	Time	Total	Vulnerability	Total	

FORM 5: Write an IO Objective statement.

1) Effect. Potential effects to meet IO objective:
2) Target.
   a. Hardware (physical targets):
   b. Software (programs):
   c. Wetware (people):
   d. Information:
3) Purpose:

4) Write IO OBJECTIVE:

FORM 6/7: Establish time phasing of IO Objectives.

FORM 8: Opposition Activities will be affected.
1) IO objective:
2) Opposition Activities that will be affected:

FORM 9: Identify the Functions that most contribute to the Opposition's conduct of the Activity.

	Contribution (.33):			Impact (.33):			Uniqueness (.33):			Total
Enemy Function	Role	Value	Total	Econ	Mission	Total	Redundancy	Recoverability	Total	

FORM 10: Identify the Effect desired on the selected Functions.

FORM 11: De-conflict the Effects desired on the selected Function.
1) Selected Function
2) De-conflict the effects:

FORM 12: Identify the Element most suitable to achieve the Effect desired.

FORM 13: Write the IO Task Statements.
1) ID the target:
2) ID the effect:
3) Select the IO capability:
4) The Why:
5) Write the IO task.
6) Objective:
7) IO task:

FORM 14: Assign the IO Tasks to the Components.

FORM 15: Identify the IO Targets.
1) Hardware:
2) Software:
3) Wetware:

4) Data:

FORM 16: Evaluate targets associated with the Function.
1) Hardware:
2) Software:
3) Wetware:
4) Data:

FORM 16A: Evaluate and targets associated to identify the ones most critical to the success.

	Contribution (.25):			Impact (.25):			Uniqueness (.25):			Vulnerability (.25):				Total
:nemy Targets	Role	Value	Total	Econ	Mission	Total	Redundancy	Revocability	Total	Access	Feasibility	Susceptibility	Total	

FORM 17: Confirm or Refine Effects desired on targets selected.

FORM 18: De-Conflict Effects desired on selected targets.

FORM 19: Identify the IO Asset.

IO Asset Number	Apportioned (Yes/No)	Assigned (Yes/No)	Allocated (Yes/No)	Deployed (Yes/No)	In-commission (Yes/No)	Availability (H/M/L)	Duration (H/M/L)	Delivery Error (H/M/L)	Probability of Effect (H/M/L)	Asset Reliability (H/M/L)	Total Score

FORM 20: COST/BENEFIT/RISK of IO Asset #2 against
1) Cost (.33):
   a. Consequences = LOW (.2)
   b. Number = LOW (.2)
   c. Value = High (.8)
2) Risk (.33):
   a. Prob. Failure = Med (.5)

b. Consequences of Failure = High (.8)
c. Capability of Compromise = LOW (.2)
d. Collateral Damage = LOW (.2)

3) Benefit (.33):
   a. Prop of Success = High (.8)
   b. Political Acceptability = MED (.5)
   c. Confidence = HIGH (.8)
   d. Impact = MED (.5)
   e. Reconstitution = LOW (.2)
4) Total: 1.815

FORM 21: Derive and write IO Sub-task.

FORM 22: Mater IO Target List.

FORM 23: MOE and Equity Review.

1) Potential Indicators of MOE:
2) Equity Review.
   a. Operational gain versus intelligence loss: Gain outweighs intelligence loss.
   b. Joint Restricted Frequency Lists: Low probability of fratricide.
   c. Security Compromise: No.
   d. No Strike: No.
   e. Service: Low.

APPENDIX B: KEY TERMS

1. Coalition/ Combined Task Force (CCTF): A military force composed of elements of two or more allied nations. (DoD)

2. Cooperative IO (CIO): When a cadre of military planners from different nations comes together to plan and execute IO during and MNF exercise or real world operation.

3. Information Environment (IE): Is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (FM 3-13)

4. Information Management (IM): Is all activities involved in the collection, filtering, fusing, processing, dissemination and use of information for CCTF operations. Information that promotes understanding of the battle space enables commanders to better formulate and analyze courses of action, make decisions, execute those decisions with adjustments to the plan as necessary, and accurately assess the operation.

5. Information Operations (IO): Are actions taken to affect adversary and influence others' decision-making processes, information, and information systems, while protecting one's own information and information systems. (FM 3-0)

6. Information Superiority: The capability to collect, process, and disseminate an uninterrupted flow of information whiles exploiting or denying an adversary's ability to do the same. (JP1-02)

7. Multi National Information Operations (MNFIO): Are actions taken to effect information, information systems, and influence decision making processes of political, military, and social entities while protecting one's own. IO spans the entire spectrum from peace, to crisis, to conflict, to restoration.

8. Military Operations other Than War (MOOTW): Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power

and occur before, during, and after war. MOOTW focus on deterring war and promoting peace while war encompasses large-scale, sustained combat operations to achieve national objectives or to protect national interests. (JP 3-07)

9. Multi National Operations (MNF): A collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance. (DoD)

10. Multi Planning and Augmentation Team (MPAT): A cadre of military planners with interests in the Asia-Pacific region capable of rapidly augmenting a multinational force headquarters established to plan and executes coalition operations in response to small-scale contingencies.

11. Small Scale Contingencies (SCC): A military operation that is either designated by the Secretary of Defense as a contingency operation or becomes a contingency operation as a matter of law (10 United States code (USC) 101[a][13]). It is a military operation that: a. is designated by the Secretary of Defense as an operation in which members of the Armed Forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States or against an opposing force; or b. is created by definition of law. Under 10 USC 101 (a)(13)(B), a contingency operation exists if a military operation results in the (1) call up to (or retention on) active duty of members of the uniformed Services under certain enumerated statutes (10 USC Sections 688, 12301(a), 12302, 12304, 12305, 12406, or 331-335); and (2) the call up to (or retention on) active duty of members of the uniformed Services under other (non-enumerated) statutes during war or national emergency declared by the President or Congress. (DoD)

12. Standard Operating Procedures (SOP): A set of instructions covering those features of operations, which lend themselves to a definite or standardized procedure without loss of effectiveness. The procedure is applicable unless ordered otherwise. (DoD, NATO)

LIST OF REFERENCES

Adams, J., (1998). *The Next World War*. New York: Simon & Schuster.

Alberts, D. A., Garstka, J.J., Hayes R. W., & Signori D.A. (2001). *Understanding Information Age Warfare*. Washington D.C.: CCRP Publication Series.

Armstrong, R. N., (1998). *Soviet Operational Deception: The Red Clock*. Fort Leavenworth, Kansas: U.S. Army Command and General Staff College.

Avent, D. D. (1996). *Military Reluctance To Intervene In Low-Level Conflicts: A "Crisis"?* Paper presented and sponsored by the U.S. Army War College's Strategic Studies Institute and The Patterson School of Diplomacy and International Commerce, University of Kentucky.

Barge, H., Davis M., Schwent, J., (2003). *Field Level Information Collaboration During Complex Humanitarian Emergencies And Peace Operations.* Monterey: Naval Postgraduate School.

Beyea, D. (2003). *Kitty Hawk Sailors Practice Good OPSEC*. Retrieved 20 November 2003 from http://www.news.navy.mil/search/display.asp?story_id=5995.

CIA Fact Book, 2003. //www.cia.gov/cia/ publications/ factbook/geos/rw.html# Intro. dated 24 October 04. Last updated 01 Aug 2003.

Chairman of the Joint Chiefs of Staff. (1997). *Joint Pub 3-61 Doctrine For Public Affairs in Joint Operations*, Washington DC: U.S. Government Printing Office.

Chairman of the Joint Chiefs of Staff. (1998). *Joint Pub 3-13 Joint Doctrine for Information Operations*. Washington DC: U.S. Government Printing Office.

Chairman of the Joint Chiefs of Staff. (2000). *Joint Pub 3-16 Joint Doctrine for Multi National Operations*. Washington DC: U.S. Government Printing Office.

Chairman of the Joint Chiefs of Staff. (2000). *Joint Vision 2020. America's Military: Preparing for Tomorrow.* Washington DC: U.S. Government Printing Office.

Chairman of The Joint Chiefs of Staff. (2000). *Standing Rules of Engagement for U.S. Forces*. *CJCSI 3121.01A Instruction.* Washington DC: U.S. Government Printing Office.

Chairman of the Joint Chiefs of Staff. (2001). *Joint Pub 3-0 Doctrine For Joint Operations*. Washington DC: U.S. Government Printing Office.

Chairman of the Joint Chiefs of Staff. (2003). *Joint Pub 1-02 Department of Defense Dictionary of Military and Associated Terms.* Washington DC: U.S. Government Printing Office.

Chairman of the Joint Chiefs of Staff. (2003). *Joint Pub 3-53 Joint Doctrine for Psychological Operations*. Washington DC: U.S. Government Printing Office.

David, V. (1996). *Civil-Military Relations and the Not-Quite Wars of the Present and Future*. Papers presented and sponsored by the U.S. Army War College's Strategic Studies Institute and The Patterson School of Diplomacy and International Commerce, University of Kentucky.

Defense Service Board. (2002). *Report of the Defense Science Board Task Force on The Creation and Dissemination of All Forms of Information in Support of Psychological Operations (PSYOP) in Time of Military Conflict.* Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

Denning, D. E. (1999). *Information Warfare and Security*. Boston: Addison-Wesley.

Department of the Air Force. (1995). *Cornerstones of Information Warfare*, Washington DC: U.S. Government Printing Office.

Department of the Army. (1978). *FM 90-2*, *Battlefield Deception*. Washington, D.C.: U.S. Government Printing Office.

Des Forges, A. (1999). *Leave None to Tell The Story, Genocide in Rwanda*. New York: Human Rights Watch.

Feil, S. R. (1998). *Preventing Genocide: How the Early Use of Force Might Have Succeeded in Rwanda*. Washington D.C.: Carnegie Commission on Preventing Deadly Conflict.

Ferroggiaro, W. (2001). *A National Security Archive, Electronic Briefing Book.* Retrieved 20 August 2001. http: //www.gwu.edu/~nsarchiv/ NSAEBB/NSAEBB53/

Gompert, D. C., Kugler, R L., & Libicki, M.C. (1999). *Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs.* Washington D.C.: National Defense University Press.

Hernandez R., Sims T. M., Borlik J. R. Jr., Phelps R., & Rush J. A. (2003). *Maintaining Credibility Within Military Public Affairs While Preserving and Participating in Military Deception*. Retrieved 27 November 2003 from http://www.ou.edu/deptcomm/dodjcc/groups/98B1/paper.htm.

Human Rights Watch/FIDH interviews, August 18 and 19, 1995; Kigali. Adopted from Des Forges, A. (1999). *Leave None to Tell The Story, Genocide in Rwanda*. New York: Human Rights Watch.

Keane, F. (1995). *Season of Blood, A Rwandan Journey*. London: Penguin Book.

Krepinevich, A. F. (1995). *War Theory*, vol. 3, *The Military-Technical Revolution: A Preliminary Assessment* Alabama: Air University Press.

Lacey, M.O., & Bill, B. R. (2001). *Operational Law Handbook*. International and Operational Law Department. The Judge Advocate General's School. Washington D.C.: U.S. Government Printing Office.

Leonhard, R. R. (1998). *The Principles of War for the Information Age,* Novato California: Presidio Press, INC.

Libicki, M. C. (1996). *What is Information Warfare*? Washington, D.C.: National Defense University.

Liotta, P.H. (2000). *To Die For: National Interests and Strategic Uncertainties.* Newport: Naval War College Press.

Louisiana State University. Retrieved 27 October 2003 from http://www.lcet.doe.state.la.us/laintech/propagan.htm.

Mclure, W. B. (2000). *Technology and Command Implications for Military Operations in the Twenty-first Century*. Center For Strategic and Air Warfare, College.

MindSim Corporation. Adapted and retrieved 22 November 2003 from http://www.mindsim.com/MindSim/Corporate/OODA.html.

MITRE Corporation. Retrieved 11 November 2003 from http://www.mitre.org/.

Morthlans, S. P. (2002). Information Operations: The Need For a National Strategy. Monterey: Naval Postgraduate School Publication. Retrieved 22 November 2003 from http://library.nps.navy.mil/uhtbin/cgisirsi/Sun+Nov+23+11:33:58+PST+2003/0/520/02Jun_Morthland.pdf.

Nichiporuk, B. (2000). *Forecasting the effects of Army's XXI Design Upon Multinational Force.* Santa Monica, California: RAND Arroyo Center.

OPSEC Organization. (2003) Retrieved 20 November 2003 from http://www.opsec.org/.

Palin, R. H. (1995). *Multinational Military Forces: Problems and Prospects*. New York: Oxford University Press.

Pacific Command. Retrieved 11 November 2003 from http://www.pacom.mil/.

Prunier, G. (1995). *The Rwanda Crises: History of a Genocide*. New York: Colombia University Press.

Pudas, T. J. (1994). *Preparing Future Coalition Commanders*. Joint Force Quarterly, Institute for National Defense Strategic Studies, Washington D.C.: National Defense University.

Raytheon. (2003). *Shortening the Sensor-to-Shooter Time Line.* Retrieved 25 November 2003 form http://www.raytheon.com/missions/precision/.

Sadeghiyan, B. (1992). *An Overview of Secure Electronic Mail*. Dept. of Computer Science, Australian Defense Force Academy.

Simon, H. A. (1976). *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization.* New York: The Free Press.

Snider, Don. (1996). *U.S. Civil-Military Relations And Operations Other Than War.* Paper presented and sponsored by the U.S. Army War College's Strategic Studies Institute and The Patterson School of Diplomacy and International Commerce, University of Kentucky.

Tzu, S. (1971). *The Art of War*. Translated by Samuel B Griffith, London: Oxford University Press, London.

Waltz, E. (1998). *Information Warfare, Principles and Operations*. Boston: Artech House.

White, J. B. (1996). *Some Thoughts on Irregular Warfare*. Washington, D.C.: reprinted from Studies in Intelligence Vol. 39, No 5.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Post Graduate School
   Monterey, California

3. Pacific Command
   Attention: John Bratton
   Honolulu, Hawaii

4. Dr. Dan Boger
   Naval Postgraduate School
   Monterey, California

5. COL Thomas Moore, PHD
   Naval Postgraduate School
   Monterey, California

6. Raymond Buettner
   Naval Postgraduate School
   Monterey, California